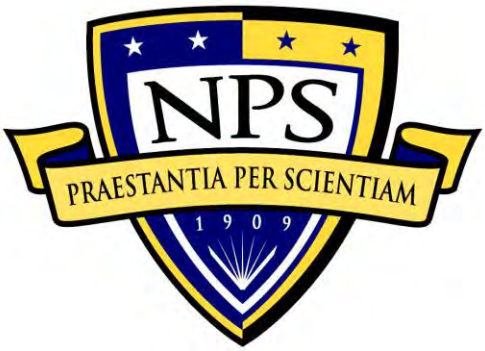


# NAVAL POSTGRADUATE SCHOOL

**MONTEREY, CALIFORNIA**

# THESIS

**THE COMMANDING OFFICER'S PERSPECTIVE ON PROTECTING SHIPBOARD IT NETWORKS**

by

Steven Zielechowski

September 2014

| | |
|---|---|
| Thesis Advisor: | Raymond R. Buettner |
| Second Reader: | Glenn R. Cook |

**Approved for public release; distribution is unlimited**

THIS PAGE INTENTIONALLY LEFT BLANK

# REPORT DOCUMENTATION PAGE

*Form Approved OMB No. 0704-0188*



| **1. AGENCY USE ONLY** *(Leave blank)* | **2. REPORT DATE** September 2014 | **3. REPORT TYPE AND DATES COVERED** Master's Thesis |
|---|---|---|

**4. TITLE AND SUBTITLE**
THE COMMANDING OFFICER'S PERSPECTIVE ON PROTECTING SHIPBOARD IT NETWORKS

**5. FUNDING NUMBERS**

**6. AUTHOR(S)** Steven Zielechowski

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
Naval Postgraduate School
Monterey, CA 93943-5000

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)**
N/A

**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

**11. SUPPLEMENTARY NOTES** The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB protocol number ____N/A____. Note: this research was not conducted in accordance with Department of Defense, Federal, and Navy Human Research Protection Regulations.

| **12a. DISTRIBUTION / AVAILABILITY STATEMENT** | **12b. DISTRIBUTION CODE** |
|---|---|
| Approved for public release; distribution is unlimited. | A |

**13. ABSTRACT (maximum 200 words)**

This thesis explores the perceived need or lack of need for an active defense system afloat (e.g., the covert analysis detection [CAD] system) to protect shipboard networks from possible cyber-attacks. As hacking methods evolve, it is likely that nation-states and terrorists will attempt to interfere with or take control of shipboard systems remotely. This thesis builds on the work of previous NPS theses that suggest the Navy consider deploying a CAD system in the Aegis Combat System to secure better the system against potential cyber intrusions or attacks. This system could covertly detect intrusions of malicious programs and track their activities and behavior, deceive the malicious software, and/or isolate it to keep it from causing irreparable harm while deceiving the attacker with regard to system status. The data would only be available to the CO and designated shipboard personnel. In order to determine a need for such a system, 10 current and former commanders afloat were surveyed. The overwhelming majority saw a need to defend ships from cyber-attacks. Most of them saw the benefit of a CAD system in the cyber defense of U.S. Navy warships. This thesis recommends the development of the CAD system for shipboard use.

| **14. SUBJECT TERMS** Covert Analysis Direction System, covert analysis detection, CAD, shipboard networks, cyber attack | **15. NUMBER OF PAGES** 135 |
|---|---|
| | **16. PRICE CODE** |

| **17. SECURITY CLASSIFICATION OF REPORT** | **18. SECURITY CLASSIFICATION OF THIS PAGE** | **19. SECURITY CLASSIFICATION OF ABSTRACT** | **20. LIMITATION OF ABSTRACT** |
|---|---|---|---|
| Unclassified | Unclassified | Unclassified | UU |

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release; distribution is unlimited**

# THE COMMANDING OFFICER'S PERSPECTIVE ON PROTECTING SHIPBOARD IT NETWORKS

Steven Zielechowski
Lieutenant, United States Navy
B.A., Villanova University, 2004

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT**

from the

**NAVAL POSTGRADUATE SCHOOL**
**September 2014**

Author: Steven Zielechowski

Approved by: Raymond R. Buettner
Thesis Advisor

Glenn R. Cook
Second Reader

Dan C. Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

# ABSTRACT

This thesis explores the perceived need or lack of need for an active defense system afloat (e.g., the covert analysis detection [CAD] system) to protect shipboard networks from possible cyber-attacks. As hacking methods evolve, it is likely that nation-states and terrorists will attempt to interfere with or take control of shipboard systems remotely. This thesis builds on the work of previous NPS theses that suggest the Navy consider deploying a CAD system in the Aegis Combat System to secure better the system against potential cyber intrusions or attacks. This system could covertly detect intrusions of malicious programs and track their activities and behavior, deceive the malicious software, and/or isolate it to keep it from causing irreparable harm while deceiving the attacker with regard to system status. The data would only be available to the CO and designated shipboard personnel. In order to determine a need for such a system, 10 current and former commanders afloat were surveyed. The overwhelming majority saw a need to defend ships from cyber-attacks. Most of them saw the benefit of a CAD system in the cyber defense of U.S. Navy warships. This thesis recommends the development of the CAD system for shipboard use.

THIS PAGE INTENTIONALLY LEFT BLANK

# TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF TABLES



-

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| ACTS | AEGIS Combat Training System |
| ADM | admiral (rank not position) |
| ADS | AEGIS Display System |
| AOR | area of operations |
| AWS | AEGIS weapon system |
| BDOC | basic division officer's course |
| BMD | ballistic missile defense |
| C&D | command and decision |
| C10F | Commander, Tenth Fleet |
| C2 | command and control |
| C4I | command, control, communications, computers, and intelligence |
| C4ISR | command, control, communications, computers, intelligence, surveillance, and reconnaissance |
| CAD | covert analysis detection |
| CAPT | captain (rank not position) |
| CARAT | cooperation afloat readiness and training |
| CAW | carrier air wing |
| CDO | command duty officer |
| CDR | commander (rank not position) |
| CG | guided missile cruiser |
| CIA | Central Intelligence Agency |
| CICWO | combat information center watch officer |
| CIP | critical infrastructure protection |
| CMAV | continuous maintenance availability |
| CMC | Commandant of the Marine Corps |
| CNA | computer network attack |
| CND | computer network defense |
| CNE | computer network exploitation |
| CNO | Chief of Naval Operations |
| CNO | computer network operations |

| | |
|---|---|
| CO | commanding officer |
| COCOM | combatant command (command authority) |
| COMMO | communications officer |
| COMPTUEX | composite training unit exercise |
| COTS | commercial-off-the-shelf |
| CRUDES | cruiser and destroyer |
| CSG | carrier strike group |
| CSO | combat systems officer |
| CVN | aircraft carrier, nuclear |
| CYBERCOM | Cyber Command |
| DDG | guided missile destroyer |
| DESRON | destroyer squadron |
| DH | department head |
| DIVO | division officer |
| DOD | Department of Defense |
| DoN | Department of the Navy |
| ECD | energy change detection |
| ENS | ensign |
| EOOW | engineering officer of the watch |
| FCS | Fire Control System |
| FFG | guided missile frigate |
| FLTCYBERCOM | Fleet Cyber Command (Navy) |
| G-C | Commandant of the Coast Guard |
| GIG | Global Information Grid |
| GMT | general military training |
| GPS | geospatial positioning system |
| IA | information assurance |
| IDC | Information Dominance Corps |
| IDCERTEX | Independent Deployer Certification Exercise |
| IP | internet protocol |
| IT | information technology |
| JP | joint publication |

| | |
|---|---|
| JTFEX | joint task force exercise |
| JWICS | Joint Worldwide Intelligence Communications System |
| LCDR | lieutenant commander |
| LCS | littoral combat ship |
| LT | lieutenant |
| LTJG | lieutenant junior-grade |
| MAJ | major |
| MCM | mine countermeasures |
| N/A | not applicable |
| NATO | North Atlantic Treaty Organization |
| NIPR | Non-Secure Internet Protocol Router |
| NIVA | Naval Integrated Vulnerability Assessment |
| NKO | navy knowledge online |
| NOC | naval operations concept |
| OJT | on the job training |
| OOD | officer of the deck |
| OPNAV | Chief of Naval Operations |
| ORTS | operational readiness test system |
| PACOM | Pacific Command |
| PC | patrol craft |
| PCU | precomissioning unit |
| PII | personally identifiable information |
| PQS | personnel qualification standards |
| RADM | rear admiral upper half |
| RDML | rear admiral lower half |
| RET | retired |
| RMS | remote mine submersible |
| S | secret |
| SCADA | supervisory control and data acquisition |
| SECNAV | Secretary of the Navy |
| SES | senior executive service |
| SIAM | situational influence assessment model |

| | |
|---|---|
| SIGINT | signals intelligence |
| SIPR | secure internet protocol router |
| SME | subject matter expert |
| SPY | AN/SPY-1 Radar System |
| SRA | specialized-repair activity |
| SSG | strategic study group |
| SWO | surface warfare officer |
| SWOS | Surface Warfare Officer's School |
| TACTOM | tactical tomahawk |
| TAO | tactical action officer |
| TS | top secret |
| TWS | tomahawk weapon system |
| U.S. | United States |
| UNCLAS | unclassified |
| UNREP | underway replenishment |
| URL | unrestricted line |
| USCYBERCOM | United States Cyber Command |
| USN | United States Navy |
| VADM | vice admiral |
| WCS | Weapons Control System |
| WEPS | weapons officer |
| WIFI | wireless fidelity |
| XO | executive officer |

# ACKNOWLEDGMENTS

First, I would like to thank my wife, Sara, for standing by me and seeing me through this thesis process. I would like to thank both Dr. Raymond Buettner and Glenn Cook for their continued support throughout this whole process. Finally, I would like to thank my family, friends, and co-workers whose continued support and encouragement were great motivators that led the successful completion of my master's thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

# I. INTRODUCTION

## A. THE NEED TO SECURE SHIP NETWORKS FROM CYBER ATTACKS

The motivation behind this thesis is a combination of the reliance on information technology (IT) and a concern to ensure the security of shipboard weapons networks. As a surface warfare officer (SWO), the security of weapons systems is of keen interest to the author. Knowing that shipboard systems are protected from cyber-attacks and infiltration by enemies (e.g., [cyber] terrorists and state actors) is critical in projecting sea power. It is critical for a commanding officer (CO) and their tactical action officers (TAOs) to know that their weapons systems are secure and reliable at all times.

In order to further the discussion, it was necessary go beyond the theories and to discuss with actual warfighters their firsthand experience in, knowledge of, and reflections on command. This information will provide a basis for future studies and potentially future cyber defense systems that will better insulate shipboard networks from cyber-attacks. This will draw on tactical knowledge that has developed over several careers at sea. This invaluable insight will help both to build upon the aforementioned writings and to develop future avenues for improving naval tactics to better defends ships at sea in the age of cyber.

## B. RESEARCH QUESTION AND METHODOLOGY

This thesis will seek to identify current and potential threats to shipboard networks that need to be addressed by consulting current and former COs of United States Navy (USN) warships. The current and future threats identified will help to further ongoing and future research in the area of cyber sensitivities of shipboard systems. As technology quickly advances, it is necessary that the Navy's defensive and offensive capabilities do as well. Discussions with those who have ultimate responsibility of these ships and the systems onboard will provide an invaluable viewpoint.

In today's age of cyber warfare, the threats that face U.S. ships are greater than in the past. As Captain (CAPT) (ret.) Wayne P. Hughes, Jr. has commented, "Technology is renowned for the way in which it changes tactics: tactical trends develop because of

technology, and tactical constants abide in spite of new technology."[1] It is necessary therefore to account for IT in creating shipboard systems and developing doctrine as advances are made in cyber technology. Potential threats include both hackers (e.g., groups like Anonymous) and nation-states. Advances in IT are beneficial to national security but also have the potential to leave users susceptible to intrusion. With U.S. ships (e.g., the littoral combat ship [LCS]), operating in coastal waters, they are increasingly susceptible to attack by our adversaries both physically and in the cyber domain. In particular, Dr. J. P. London in *Proceedings Magazine* cites Chinese advances in cyber,

> One significant investment is reported to be a 1,100-person cyber operation at Hainan Island (complete with a James Bond-style submarine cave), which also is home to some key Chinese military units. Canadian researchers have found that a number of cyber-attacks originated there; US Navy ships near the island have been harassed.[2]

As other countries make advances in cyber, the Navy should anticipate needing to implement critical upgrades to network security and doctrinal adjustments more frequently to counter the ever-changing cyber "battle field." Ships operating close to shore may be most susceptible to active cyber-attacks, while all ships would be susceptible to passive cyber-attacks by infected hardware or software.

With the inherent difficulty of tracking down the source of cyber-attacks in order to curtail future attacks, it is imperative to be proactive and protect network infrastructures from potential intrusion. Unprotected shipboard networks could potentially give hackers or rogue nation-states access to naval weapons systems, global positioning systems, operational plans, etc. It is likely that events such as the selling to Department of Defense (DOD) of counterfeit Cisco routers[3] will be attempted again in the future by criminal organizations or countries. Questions arise not as to whether

---

[1] Wayne P. Hughes, *Fleet Tactics and Coastal Combat* (Annapolis, MD: Naval Institute Press, 2000), 228.

[2] J. Landon, "Made in China," *Proceedings Magazine* 137, no. 298, April 2011, accessed February 22, 2014, http://www.usni.org/magazines/proceedings/2011-04/made-china.

[3] Stephen Lawson and Robert McMillan, "FBI Worried as DoD Sold Counterfeit Cisco Gear: By Tampering with Networking Equipment, Spies Could Open up a Back Door to Sensitive Military," InfoWorld, accessed February 22, 2014, http://www.infoworld.com/d/security-central/fbi-worried-DOD-sold-counterfeit-cisco-gear-266.

shipboard networks are currently impenetrable to all cyber-attacks but if they are capable of detecting intrusion on the network and of being reconfigured quickly to counter. Additionally, are current shipboard systems susceptible to real time cyber-attacks? Are all measures being taken to ensure that hardware and software that has been tampered with is being identified prior to installation to avoid future counterfeit products from making their way aboard ships? This thesis explores the nature of the cyber threat to U.S. warships through the conduct and analysis of a survey of current and recent COs. The potential utility of a notional defensive system is also explored.

## C. THESIS OUTLINE AND RECOMMENDATIONS

Chapter I has introduced the topic and the methodology for this thesis. Chapter II is a literature review of previous theses, scholarly writings, and books. The purpose is descibe the foundation for this thesis and the associated survey of COs afloat and the sensitivity of a naval warship to cyber-attack. Chapter III lays out how the survey was developed and formatted. Additionally, it looks at the potential for identifying areas of concern. Chapter IV analyzes the results of the 10 surveys. Finally, Chapter V summarizes the findings of this study as well as presents areas for future research to ensure protection of shipboard networks from future cyber-attacks.

THIS PAGE INTENTIONALLY LEFT BLANK

# II. RELATED RESEARCH AND WRITINGS

## A. DEFINITIONS

Cyberspace has come to the forefront over the past decade as having vast benefits for both government and civilian sectors while at the same time having potential negatives to the security of networks. There are several definitions for cyberspace. Richard A. Clarke defines it as "all of the computer networks in the world and everything they connect and control."[4] Current Chief of Naval Operations (CNO) ADM Johnathan Greenert says, "Cyberspace will be operationalized with capabilities that span the electromagnetic spectrum–providing superior awareness and control when and where we need it."[5] Joint Publication (JP) 1-02 defines it as "A global domain within the information environment consisting of the interdependent network of IT infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[6]

Words that arise in any discussion of cyber and the DOD that can be used to discuss the protection of Navy shipboard networks are defined as follows according to JP 1-02:

- Cyberspace Operations—The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.[7]
- Global Information Grid (GIG)—The globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.[8]

---

[4] Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security* (New York: HarperCollins Publishers, 2010), 70.

[5] Johnathan Greenert, *CNO's Sailing Directions*, 2011, http://www.navy.mil/cno/cno_sailing_direction_final-lowres.pdf, 2.

[6] Department of Defense, *Department of Defense Dictionary of Military and Associated Terms* (Joint Publication 1-02), 2010, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf, 64.

[7] Ibid., 64.

[8] Ibid., 111.

- Information Assurance (IA)—Actions that protect and defend information systems by ensuring availability, integrity, authentication, confidentiality, and nonrepudiation.[9]

## B. POLICY AND GUIDANCE

October 2007's *A Cooperative Strategy for 21st Century Seapower* points out "The ability to operate freely at sea is one of the most important enablers of joint and interagency operations, and sea control requires capabilities in all aspects of the maritime domain, including space and cyberspace."[10] This was the vision of former CNO Admiral (ADM) Gary Roughead. Both the Commandant of the Marines Corps (CMC) and the Commandant of the Coast Guard (G-C) also recognized the importance of cyber in the maritime domain. By presenting it in a joint roadmap for the way ahead in the next century, they are ensuring it will be a consideration in all future doctrine and mission planning.

ADM Roughead further amplified the importance of cyber in the 2010 *Naval Operations Concept* (NOC). "The interrelationship between sea control and power projection mandates that the Naval Service possess capabilities and capacity to concurrently shape conditions in the maritime, space and cyberspace domains, sufficient to accomplish the Nation's defense strategy."[11] He sees it as a vital key to conducting sustained combat operations in support of the U.S. maritime security.

The NOC also identifies one of the current challenges facing the Navy to be "Technologies that disrupt space and cyberspace capabilities, particularly command, control, communication, computer, and intelligence (C4I) systems."[12] This thesis seeks to identify some of these potential disruptors and discuss both potential offensive and defensive measures that can be taken. In order to counter these threats,

---

[9] Ibid., 127.

[10] U.S. Marine Corps, U.S. Department of the Navy, and U.S. Coast Guard, *Cooperative Strategy for 21st Century Seapower*, accessed March 28, 2014, http://www.navy.mil/maritime/MaritimeStrategy.pdf, 13.

[11] Ibid.

[12] Ibid., 53.

> Naval forces will deploy and employ redundant systems to maintain command and control [C2] of dispersed forces in the face of such threats, and will maintain proficiency in retaining the operational and tactical initiative when communications and information systems are degraded or denied.[13]

Not only are reliable systems a factor, but watchstander proficiency and training are factors in countering potential cyber threats.

There is a need to properly utilize current systems and employ future systems that can withstand or recover quickly from an intrusion by a hacker or non-friendly state actor. The Navy needs to have "superior warfare systems, which provide robust integrated air and missile defense, including ballistic missile defense; effective undersea warfare; and flexible network-centric attack options using organic and off-board weapons."[14] Shipboard and ashore computer networks that allow COs to employ weapons, safely navigate the maritime domain, and ensure the safety of their crews must be available 24 hours a day. This is specifically achieved through "Cyberspace Superiority, enhanced by sound IA practices, which ensures that critical networks are defended and full spectrum computer network operations effectively support widely dispersed naval forces engaged in sea control operations."[15]

Not only is cyber recognized as an asset and a threat by the CNO, but also the Secretary of the Navy (SECNAV) the Honorable Ray Mabus sees it as such. In written testimony in February 2010 to Congress, he stated,

> The ships and aircraft of the Navy and Marine Corps are unmatched at sea and over land. Our precision munitions, networked targeting systems, armored vehicles, stealth technology, and unmanned vehicles are advanced systems that define the leading edge of warfare in all domains.[16]

---

[13] Ibid., 54.

[14] Ibid., 56.

[15] Ibid., 57.

[16] "Written Congressional Testimony of the Honorable Ray Mabus Secretary of the Navy February 24, 2010," 2010, http://www.navy.mil/navydata/people/secnav/mabus/posture_statement_2010, 15.

The systems employed by the Navy require cyber security to remain online and effective. If shipboard networks were easily penetrable, there would be little to no reliability in their effectiveness. It is critical to protect these systems from intrusion and to be prepared to counter quickly any breach.

Cyberspace will be operationalized with capabilities that span the electromagnetic spectrum–providing superior awareness and control when and where we need it. In 2011, then CNO ADM Gary Roughead acknowledged the need for cyber superiority within the Navy in his CNO Guidance for 2011. He did so through two specific actions. First, he designated a Deputy CNO for information dominance (OPNAV N2/N6); and second, he established Fleet Cyber Command/Commander Tenth Fleet (FLTCYBERCOM/C10F).[17] FLTCYBERCOM reports directly to United States Cyber Command (USCYBERCOM). This further recognition of the importance of cyber will allow for advances in protection from upcoming threats both at sea and ashore. It is critical that threats be not only identified but also understood. These two offices will afford COs the ability to reach back to shore while deployed to address any threats. These threats may be immediate ones that they are facing at sea or may be actionable intelligence known ashore. This also builds on his declaration in the NOC that "We will institutionalize and mature the Information Dominance Corps [IDC] and build its reputation as an elite cyber force."[18] Roughead saw the importance of addressing current and future threats to the Fleet.

## C. PREVIOUS THESES

Over the years, several Naval Postgraduate (NPS) theses have discussed potential cyber security threats and sensitivities to naval networks as well as potential approaches to countering them. In 2000, Lieutenant (LT) Richard J. McConnell discussed the use of wireless networks aboard ships. He touted the benefits of wireless as seemingly infinite. The idea was to implement the usage of wireless devices in order to maintain readings of shipboard equipment. The thesis built on the experience of the Navy's Smart Ship

[17] Gary Roughead, "CNO Guidance for 2011," 2010, http://www.navy.mil/features/CNOG%202011.pdf, 6.

[18] Ibid.

Program. The thesis's conclusion was that future research should evaluate newer technologies as they become available. An area overlooked though, as cyber technologies continue to advance, is security and sensitivities to hacking or disruption of systems actively or passively by either nation-states or terrorists. It is necessary to improve capabilities while maintaining a secure environment.

In 2004, Major (Maj) Dennis J. Hart developed a potential checklist for protecting Supervisory Control and Data Acquisition (SCADA) systems. "A SCADA system is the software that controls networks such as electric power grids."[19] He acknowledged the sensitivity of Navy systems, particularly to potential terrorist attacks, "Al Qaeda computers contained information about SCADA devices and how to hack them."[20] At that time, the Navy relied on an internal process to ensure cyber security. Also according to Hart,

> DoN's [Department of the Navy's] CIP [Critical Infrastructure Protection] Program strategy is the Naval Integrated Vulnerability Assessment (NIVA) process. This process is used to identify and evaluate critical sensitivities and single points of failure by helping to protect mission critical cyber and physical mission essential infrastructures.[21]

The Navy requires the use of shipboard and shore based systems in order to function. These include "Electric power and telecommunications facilities [that] make extensive use of SCADA systems."[22] The Navy also utilized SCADA Systems onboard Mine Counter Measure (MCM) ships to improve the engineering plant. This was done with a mix of commercial-off-the-shelf (COTS) hardware and 'intelligent software.'[23] The key takeaway was that in order to protect naval assets not only does

> More work [need] to be done in encouraging commercial entities to treat seriously the threat posed by cyber-attacks to process control networks.

---

[19] Clarke and Knake, *Cyber War*, 34.

[20] Dennis J. Hart, "An Approach to Vulnerability Assessment for Navy Supervisory Control and Data Acquisition (SCADA) Systems" (master's thesis, Naval Postgraduate School, 2004), 7.

[21] Ibid., 12.

[22] Ibid., 14.

[23] Ibid., 11.

> [But] the DoN also needs to examine its own process control networks in order to ascertain and mitigate that threat as well.[24]

In 2007, LT Rodrick A. Tester conducted research on the potential sensitivities of ships in port to cyber-attacks. Drawing motivation from both John Serbian's, then Information Operations Issue Manager for the Central Intelligence Agency (CIA), statements to Congress in 2000 and Dr. Dorothy Denning's book *Information Warfare and Security*, he established a scenario to determine the likelihood of a successful cyber-attack against a U.S. warship.[25] The author went into detail about the potential entities that may attack a shipboard network as well as the potential methods they could employ. This thesis proves a useful foundation for knowledge of potential cyber threats as it provides a discussion of relevant terminology. The ultimate conclusion of the thesis was that "The [Situational Influence Assessment Module (SIAM)] model showed that even with all security tools in place, a ship is still susceptible to attack [by viruses and worms], however, the risk is much less with the tools in place."[26] In order to thwart potential hackers, it is imperative at the least to ensure a firewall and up-to-date anti-virus program are installed in all shipboard networks. This take away in conjunction with doctrinal requirements will help deter cyber threats and minimize actual cyber-attacks.

The covert analysis detection (CAD) system concept has been looked at by the Program Executive Office Integrated Warfare Systems (PEO IWS) as well as in student thesis work. Most recently, thesis research has been conducted on a CAD system. A previous NPS thesis is LT Orenthal G. Adderson and LT Kristy A. Wood's "A Qualitative Analysis of Strategic Capabilities for a Covert Analysis Detection System Onboard an AEGIS Class Ship." Adderson and Wood defined a CAD system as, "a sensor or sensor system that can covertly capture incoming and outgoing data while analyzing and maintaining control of the data."[27] And stated, "The use of a CAD system

---

[24] Ibid., 40.

[25] Rodrick A. Tester, "Risk of Cyber Attack to Naval Ships in Port Naval Station Everett: A Model Based Project Utilizing SIAM" (master's thesis, Naval Postgraduate School, 2007), 35.

[26] Ibid.

[27] Orenthal G. Adderson and Kristy A. Wood, "A Qualitative Analysis of Strategic Capabilities for a Covert Analysis Detection System Onboard an AEGIS Class Ship" (master's thesis, Naval Postgraduate School, 2010), 5.

may help to increase the overall awareness about attackers while sustaining peak levels of combat readiness through remaining discrete while protecting our own information systems."[28] This research builds upon the SIAM model as well as focusing on the risk to AEGIS equipped warships. In 2009, Capt Derek A. Filipe looked at the usage of energy change detection (ECD) on signals intelligence (SIGINT). This study looks at a technology that could one day be used against U.S. naval assets afloat. Technology such as this should be considered when discussing potential threats.[29]

In March 2010, Adderson and Wood researched the benefits of incorporating a CAD system in conjunction with the AEGIS Weapons System (AWS) onboard Arleigh Burke class guided missile destroyers (DDGs) and Ticonderoga class guided missile cruisers (CGs) given the ever-growing threat of cyber-attacks. They point out that threat is not a direct threat but rather indirect due to AEGIS being "bridged with other IT systems in order to provide critical data regarding the status of weapon systems and related operations."[30] This demonstrates the importance for COs and operators to be cognizant of the interoperability of systems across the shipboard network to ensure they are protected at all times. They describe the complexity of the AEGIS system, comprised of seven different programs: AN/SPY-1 Radar System (SPY), Command and Decision (C&D) System, Weapons Control System (WCS), Fire Control System (FCS), AEGIS Display System (ADS), Operational Readiness Test System (ORTS), and AEGIS Combat Training System (ACTS). The complexity of this system requires a subject matter expert (SME) who will be able to evaluate and understand data produced by the CAD system and report attacks and intrusions to the CO quickly in order to allow for an appropriate response as well as strengthen the protection mechanisms in place.

The answer is not simply to install commercially available IT software and hardware as soon as it is released. The authors, referencing a discussion held during their research, state that "Warfare systems are built using faster, cheaper open architecture

---

[28] Ibid., 5.

[29] Derek A. Filipe, "Energy Change Detection to Assist in Tactical Intelligence Production" (master's thesis, Naval Postgraduate School, 2009).

[30] Adderson and Wood, "A Qualitative Analysis of Strategic Capabilities," 2.

COTS computers made from sensitive technology that can be attacked and exploited by many programmers and unsophisticated users."[31] This requires a combination of both trained operators and managers that know what threats to look for as well as reliable software and hardware protections in place for shipboard networks. System managers who are up-to-date with the latest cyber threats can keep their fellow sailors apprised of potential threats and of what to look for while operating their respective system.

Historically, AEGIS, as well as other shipboard systems, has been viewed as a stove-piped system that operates as a stand-alone system and is not as sensitive as systems directly connected to a network. However, as systems are upgraded, helping to extend their lifecycle, they are becoming less stove-piped and as a result becoming potentially more sensitive to cyber-attack. "Many AEGIS components can be considered a stove-piped system; however, system updates are aiding it in gaining the fundamental characteristics of an open architecture."[32]

The inherent sensitivities of open architecture systems require COs to be informed of the latest, emerging threats to their shipboard systems. The CAD system as proposed allows COs to maintain watch on their ship's AWS as well as options when faced with a cyber-attack. "In a tactical environment, a CO could choose to respond to an incident, isolate his/her AWS network or continue to monitor the attacker through the use of active deception."[33] The discussion and potential implementation of this cyber-attack monitoring system shows the recognition of an additional front in warfare that is cyberspace. A proactive approach towards cyber sensitivities by applying the CAD system to other shipboard systems will better prepare COs for the next generation of warfare in the Information Age. While the AWS is extremely critical and could prove the most dangerous if infiltrated by adversaries, other shipboard systems (e.g., navigation, communications, and engineering) could also negatively affect a ship in a combat situation if penetrated by an adversary.

---

[31] Ibid., 44.

[32] Ibid., 46.

[33] Ibid., 50.

Their conclusion is that there are potential benefits in implementing a CAD system aboard AEGIS DDGs. According to Adderson and Wood, "Implementing a CAD system, with the proper training for the proper personnel, would give the CO the ability to focus on stealthy data capture, control and ability to conduct analysis."[34] Their findings also recommend assigning the communications officer (COMMO) as the one in charge of overseeing the CAD system, the justification is that it gives the system the oversight of an officer as well as someone that works directly with the affected systems. This would allow it to be either a collateral duty or a direct responsibility of a junior officer who will be able to keep the chain of command and ultimately the CO informed of any potential or active threats to his or her shipboard networks. This setup also recognizes the need to have more than one person monitoring the ship's critical networked systems. It is understood that the CO is ultimately responsible for the ship and its crew, but it is naïve to assume or to expect that he or she would be looking solely at all the individual systems firsthand. The implementation of CAD-like systems in parallel to weapons, communications, and navigation systems is a step in the right direction to better protecting those systems that are potentially sensitive to cyber-attack by adversaries.

Another thesis in March 2010 by Lieutenant Commander (LCDR) Sean M. Andrews, entitled "Optimizing C4ISR [command, control, communications, computers, intelligence, surveillance, and reconnaissance] Networks in the Presence of Enemy Jamming," also looked at potential network sensitivities.[35] His motivation was that "Today, the delivery of weapons by United States Navy [USN] air and surface forces is dependent upon critical target location information that is often provided to weapons and platforms by third party sensor systems forming our network."[36] This discussion acknowledges an inherent sensitivity of shipboard systems at the hardware level, which potentially leaves systems open to infiltration by adversaries. He presents a six-step kill chain comprised of "Find, Fix, Track, Target, Engage, and Assess."[37] There is the

[34] Ibid., 75.

[35] Sean M. Andrews, "Optimizing C4ISR Networks in the Presence of Enemy Jamming" (master's thesis, Naval Postgraduate School, 2010).

[36] Ibid., 1.

[37] Ibid.

possibility that an adversary infiltrates any one of these steps and false information is sent back to the ship. The results could be a missed target, an unidentified target, or a faulty assessment. The impact of any of these is that a CO's ability to conduct sustained combat operations will be degraded. This could allow an adversary to either flee the area or counterattack the ship.

One potential threat he points out by referencing an article on jamming,

> Radio broadcasts or radio messages can be jammed by beaming a more powerful signal on the same frequency at the area in which reception is to be impaired, using carefully selected noise modulation to give maximum impairment of intelligibility of reception.[38]

This type of threat is higher when ships are operating close to shore given that adversaries would be able to jam while hidden amongst the local infrastructure. Given these are the areas where newer ships (e.g., LCSs), will be deployed, it is imperative to discuss how better to protect shipboard networks from being jammed. This thesis involved modeling the effects of jamming on various steps throughout the kill chain.

The results showed how best to strengthen the kill chain in order to lessen the likelihood of jamming. According to Andrews:

> By implementing electronic countermeasures, modifying node locations and configurations, and strengthening the communications network through additional links, we have been able create a network which is less sensitive and more robust in terms of its effectiveness against an enemy's ability to attack.[39]

This research reinforced the importance of utilizing countermeasures to thwart a potential attack in addition to implementing safeguards to improve network security. Using the results of this experiment and others that test the effectiveness of shipboard networks, COs can better prepare and defend their ships against both active and passive attacks on their networks, which may cripple their ability to communicate with allies or launch missiles when necessary.

---

[38] John Markus and Paul J. DeLia, "Jamming," AccessScience, accessed March 22, 2014, http://accessscience.com/content/Jamming/358300.

[39] Sean M. Andrews, "Optimizing C4ISR Networks in the Presence of Enemy Jamming," 41.

These aforementioned theses all touch on various aspects of cyber and its potential effects on how COs defend their ships during peacetime and sustained combat operations. It is crucial to reflect on these previous studies as the discussion progresses on how best to defend weapons systems and other networked systems on ships from infiltration by potential adversaries (i.e., both nation-states and terrorists). In order to build upon these previous studies and experiments, it is imperative to reach out to the warfighters. Consequently this research emphasizes discussion with COs about what has and is 'keeping them up at night' as far as actual and potential threats to their shipboard systems. This will allow future researchers opportunities to focus their efforts on what are seen as actual and probable threats to ships at sea.

## D. ARTICLES

Michael Brown's work "Navy Operations to Achieve Military Power in Cyberspace: A Draft Concept for Navy Computer Network Operations"[40] furthers the discussion of the Navy in cyberspace. He presents the Tomahawk cruise missile AN/BGM-109E as a weapon that receives both pre-flight and in-flight data from several sources (e.g., warships) and that depends on computer network operations in order to complete its mission.[41] He addresses the need to maintain information superiority to avoid an "adversary [being] able to block or manipulate targeting, guidance, or command and control [C2] data to turn the TACTOM [tactical Tomahawk] against U.S. forces or civilian populations."[42] The threat is explained that as the U.S. advances in technology and security, it is only a matter of time before other governments or even terrorists are able to utilize the same technology and circumvent cyber security mechanisms in place. The Navy's ability to secure its weapon systems from physical intrusion are understood and addressed aboard warships. As the cyber activity increases and becomes an arena for potential military action, it is critical that the Navy protects its weapons, navigational, and

[40] Michael A. Brown, "Navy Operations to Achieve Military Power in Cyberspace: A Draft Concept for Navy Computer Operations," *Military Perspectives on Cyberpower*, ed. Larry K. Wendt, Charles L. Barry, and Stuart H. Starr (Washington, DC: National Defense University, 2009).

[41] Ibid., 74.

[42] Ibid., 74–75.

communications systems afloat. It is not a matter of if an adversary can infiltrate a ship at sea's systems but rather when will they attempt a cyber-attack.

Brown recognizes the need for commanders afloat to be able to "reach back" to shore and reach out to others afloat to make informed decisions (e.g., ensuring the correct targeting data is input into weapons systems).[43] He also states that shore-based commanders must be able to reach out to the fleet. This back and forth ability assures that combatant commanders (COCOMs) are able to have real-time information and be able to direct attacks (e.g., missiles are directed at the right targets). Brown sums up this give-and-take information sharing between commanders afloat and ashore with the COCOMs by saying, "This reciprocal access development capacity is critical for the synchronization of CNO (computer network operations) with theater operational plans and bringing CNO (computer network operations) in phase with the combatant commander's battle rhythm."[44] For this reason, it is imperative that potential cyber threats to ships be addressed.

The Information Age requires the Navy to look beyond physical threats and address those in cyberspace. As IT advances, it will be even more crucial for the Navy to be able to defend against cyber-attacks. Coordination between members of the IDC ashore and afloat will allow COs to ensure their networks and systems afloat are protected against potential threats. This can be done "by fusing all-source intelligence, network attack analysis, and known threat profiles to identify threat indicators and develop defense strategies to counter adversary attempts to degrade Naval operations."[45] Current and future threats to networks require coordination to defend and protect them.

Bringing together information gathered of potential threats allows for active computer network defense (CND), not just passive CND, with firewalls and antivirus software. The ability to defend a ship from a cyber-attack is just as critical as defending it from a physical attack by another ship or aircraft. The amalgamation of various computer

[43] Ibid., 76.

[44] Ibid.

[45] Ibid.

network exploitation (CNE) data available across the DOD's GIG allows the Navy, as well as the other services, to operate with real time data. Brown claims, "By synchronizing Navy CNE, CNA (computer network attack) and CND capabilities, we will shift from a react/report/repair response to an active prove/predict/prepare defense."[46] This 'shift' from reactive to proactive allows for networks and weapons systems protection and ensures they are online and available when needed. Ensuring reciprocal data and threat sharing allows for further integration within strike groups and with other assets.

The "Information Assurance [IA] for Network-Centric Naval Forces" presents findings from the CNO's Strategic Study Group (SSG) XXVII. The Group determined "cybersystems to be a critical component of a future commander's warfighting capability—comparable to the propulsion, weapons, and logistical systems."[47] This finding further emphasizes the growing role of cyber in 21st century warfighting. The recommendation of this group was that "commanders must be thoroughly trained and tested in all aspects of the information systems onboard their ships, submarines, aircraft, unit combat operations centers, and carriers, from both a maintenance and an operational perspective."[48] The need here is to incorporate IT training into the professional training of officers as they rise through the ranks. Potential places for it are on the job training (OJT) by inclusion of line items in both the combat information center watch officer (CICWO) and TAO personnel qualification standards (PQS). This would promote immediate knowledge of potential cyber threats afloat and required immediate actions by watch standers. Other options include at the schoolhouse level by including cyber into the appropriate curricula at Surface Warfare Officer School (SWOS) in Newport, Rhode Island. At the Flag level, cyber training could be achieved by "taking full advantage of the IT program established by the DoN for senior personnel, such as the Navy Flag and Senior Executive Service (SES) IT programs, to address cyber defense and other IA

---

[46] Ibid., 7.

[47] Committee on Information Assurance for Network-Centric Naval Forces and National Research Council, *Information Assurance for Network-Centric Naval Forces* (Washington, DC: The National Academies Press, 2010), http://www.nap.edu/catalog/12609.html, 68.

[48] Ibid.

topics."[49] The most important inclusion of cyber in the training pipeline according to this study is in the training for prospective COs because "The commander must be able to include integration of cyberwarfare (defensive and offensive) operational strategies with corresponding tactics into their warfighting operations and plans."[50] It is imperative for COs to define their objectives for preventing and combating CNE by adversaries in their Guidance to their sailors. The officers involved with SSG XXVII found cyber to be of the same importance to combat systems, operations, and engineering due to its potential impacts to the safety of a ship.

There are already a few examples of the potential dangers that can arise in cyberspace and affect the Navy. Richard M. Crowell's paper "War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare" cites a 2006 incident where a dissatisfied USN contractor attempted to plant viruses on five computers at the Navy's Naples-based European Planning and Operations Command, but only two of the five were affected. According to Crowley, "Had the other three computers been knocked offline, the network that tracks U.S. and NATO [North Atlantic Treaty Organization] ships in the Mediterranean Sea and helps prevent military and commercial vessels from colliding would have been shut down."[51] This example highlights the need for COs not only to be prepared for external cyber threats, but also for the potential internal attack by a trusted agent.

Center for Naval Analysis' March 2011 document "The Navy Role in Confronting Irregular Challenges" discusses the need for the Navy to be able to respond using cyber technologies. Given the relatively new advent of cyber-attacks and expertise needed to conduct them makes them an "irregular challenge." Their key point is "the

[49] Ibid.

[50] Ibid.

[51] Richard M. Crowell, *War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare*, accessed March 23, 2014, http://www.dtic.mil/dtic/tr/fulltext/u2/a514490.pdf.

need to maintain effective computer network defenses are important in CIC operations since irregular adversaries may use the internet for information dissemination and computer network attack."[52]

## E. BOOKS

Richard A. Clarke's book *Cyber War* covers many issues associated with cyber in depth. He discusses the formation of cyber command (CYBERCOM). As a cautionary reminder, he recalled how the Navy supplemented its Smart Ship program with COTS (i.e., Windows NT). The result of using proprietary software was that the shipboard personnel did not have access to the code to fix errors. The result was that whenever the system crashed the ship became a floating office building. Without a backup or redundant system, everything came to a standstill from the bridge to the engineering plant.[53] This example highlights the need to look thoroughly at all available options to protecting and operating shipboard networks. COTS systems have benefits but these must be weighed against potential risks as well as sensitivities that may allow outsiders access to naval networks.

## F. SUMMARY

The preceding theses, policies, articles, and books have shown areas for growing concern due to the exponential growth of and reliance on cyber over the past decade. Areas for improvement for the Navy include short-term fixes and long-term implementations. There needs to be a balance between COTS and proprietary Navy or DOD hardware and software aboard U.S. Navy ships. Advances are necessary to protect shipboard networks from cyber intrusion and attacks by a range of adversaries from the disgruntled IT professional to unfriendly state actors. Modeling potential attacks using DOD and other governmental cyber methods in parallel will allow proactive software and hardware designs as well as doctrinal changes.

---

[52] Center for Naval Analysis, "The Navy Role in Confronting Irregular Challenges Implementing the Navy Vision for CIC," March 2011, accessed March 28, 2014, http://www.cna.org/sites/default/files/research/The%20Navy%20Role%20in%20Confronting%20Irregular%20Challenges.pdf.

[53] Clarke and Knake, *Cyber War*, 140–141.

THIS PAGE INTENTIONALLY LEFT BLANK

# III. SURVEY DESIGN AND PURPOSE

A survey was designed to gather data from current and former COs afloat regarding the need (or lack thereof) for an active defense system (e.g., the CAD system) to protect shipboard networks from possible cyber-attacks and increase the tactical flexibility of the CO. As hacking methods evolve, it is likely that nation-states and terrorists will attempt to interfere with or take control of shipboard systems remotely. While there has been some research on potential cyber deterrence methods to protect ships-at-sea, there has not yet been specific steps taken to provide COs afloat with active shipboard measures for their deployment.

Building upon previous research, the next logical step in exploring the potential utility of the CAD system was determined to be surveying current and former COs afloat. This would allow the discussion to include those afloat who would potentially benefit the most from the technology.

A 26-question survey was created (Appendix A) and revised (Appendix B) to explore a CO at sea's understanding of cyber threats on their ship and crew better. In order to keep the survey objective, the participants were selected at random on a voluntary basis. No personally identifying information (PII) was collected. The survey's intent, like this research, was focused on the perceived need for the CAD system or a similar system and was not about the COs' themselves.

This survey was designed to be administered to those that have served, as COs afloat in the U.S. Navy at any rank from lieutenant (LT) through captain (CAPT). The reason for not including the ranks of ensign (ENS), lieutenant junior-grade (LTJG), rear admiral—lower half (RDML), rear admiral—upper half (RADM), vice admiral (VADM), and ADM is that there are currently no command-at-sea opportunities at these ranks. Narrowing this initial survey creates a baseline from which to relate future surveys of flag officers, junior officers, warrant officers, and enlisted service members. The main target of the survey was SWOs.

The first section asked for 'General Information.' This included rank (at the time of command afloat), ship type, experience in Weapons Department or Combat Systems Department, Ballistic Missile Defense (BMD) capable platform or not, and number of at-sea commands. This section of questions helped to formulate the demographics and better understand the responses. The ranks ranged from LT to CAPT. The reason for the range of ranks is due to patrol craft (PC) captains being LTs and CG captains being CAPTs. This allowed for a wide swath of experience to feed into the survey.

Command-at-sea means the individual has ultimate responsibility for the safety of the ship and its crew. This experience is unparalleled at any other level of responsibility, "(a)s a result of this sort of sweeping power within the … Navy, some refer to command of a … U.S. naval warships as the 'last great monarchy in the world.'"[54] This audience should have the keenest insight into which systems are most sensitive and if compromised by cyber warfare techniques would have a negative impact on national security. Their experiences of command including deployments and training exercises (e.g., Composite Training Unit Exercise [COMPTUEX] and Joint Task Force Exercise [JTFEX], will provide insight to shipboard systems). During both real world and simulated scenarios, COs afloat are faced with degradations of various systems. These experiences allow them to speak to which systems are most sensitive to attack as well as to which are mission critical.

This initial survey was not distributed to junior officers at the department head (DH) or division officer (DIVO) level. This was because while they have a general knowledge based on their various qualifications (e.g., officer of the deck [OOD], SWO, engineering officer of the watch [EOOW], and TAO); their in-depth knowledge is usually limited to their respective department or division. Further studies should look to these two audiences, (i.e., DHs and DIVOs) for further insight into specific systems deemed sensitive to cyber-attacks. An example would be that if the Tomahawk Weapons System (TWS) is determined to be susceptible to attack, weapons officers (WEPS) and strike officers should be surveyed to determine specific weaknesses and potential remedies.

---

[54] Glenn Sulmasy, *The National Security Court System: A Natural Evolution of Justice in an Age of Terror* (Oxford: Oxford University Press, 2009), 17.

Flag officers were not specifically included in this initial survey because their perspectives, as demanded by their positions, are different from those of COs afloat. Their being away from command-at-sea to fill other positions (e.g., Strike group commander or any of a variety of administrative billets) may date their opinion of what systems are most sensitive. Reasons for this may be advances in technology to protect systems or in systems being replaced. Further studies should address strike group commanders to determine what they have seen during deployments and various exercises. In addition, regional commanders can speak to regional threats to systems that may need addressed (e.g., Pacific Command [PACOM]).

Ship types included aircraft carriers (CVN), amphibious ships, CG, DDG, frigate (FFG), MCM, patrol coastal ships (PC), LCS, and other. The goal for this question is to consider all potential surface commands-at-sea.

Asking whether the individual had experience in weapons or combat systems departments helped determine if they had firsthand knowledge or experience with weapon systems (e.g., AWS found on CGs and DDGs). The reason for this interest is because while navigation and engineering systems if compromised will bring potential immediate damage to the ship itself and potentially those in the immediate vicinity, a compromised missile system may result in the inadvertent launching of weapons. This could be as severe as the launching of missiles at land-based facilities of another nation or even the U.S. The potential for irreparable damage to another nation's infrastructure or relationship with the U.S. makes the sensitivity of weapons systems to cyber-attack of particular interest.

The majority of COs afloat should have experience with other potentially critical systems that may be interfered with by unfriendly nations or terrorists. Navigation systems are learned in depth while qualifying for OOD and this knowledge is further refined by standing the watch and assisting other officers in their learning of the system. Shipboard engineering systems are also learned through various training requirements, in order to qualify as a SWO a requirement is a basic PQS on the ship's engineering plant. Additionally, a career wicket that must be met is an EOOW qualification. This qualification requires an individual be able to respond to any potential engineering

casualty quickly. In addition, in port watches such OOD and command duty officer (CDO) require knowledge of the engineering systems in the event of a casualty or emergency because the majority of the crew is not onboard after hours. It is understood that by the time of command-at-sea, an individual has a certain level of engineering, navigation, and communications knowledge.

The number of at-sea commands held by an individual highlights their overall knowledge of what it takes to maintain the safety of the ship and its crew while underway. A person with zero at-sea commands may be able to speak to potential cyber threats based on readings, second-hand knowledge from discussions, or from their tours at-sea as the executive officer (XO), a DH, or a DIVO. This is not to say their experiences and insights are not valuable, rather for this initial development of a baseline, differentiation is helpful since the target audience is those with command at-sea experience. At the opposite end is "four or more" this is because these numbers would be outside of the normal career path. The average is two (i.e., command and major command). Three is possible in the case where a CO is relieved and a CDR or CAPT is taken from staff duty to replace him or her for some period until the relieved CO's relief reports aboard. The knowledge and insight may vary amongst COs afloat based on their number of at-sea commands and in order to see if this is the case, this question is asked.

A series of follow-on questions to the number of commands seeks to determine further, how the experience and environment of command determines what is seen as a critical system. The questions look at the number of and type of deployments, homeport, areas of operation, and was it a precomissioning unit (PCU)/active unit/decommissioning unit. All these factors may shape what is seen as the most sensitive system, what the potential threats to the systems are, and potential ways to address them. An example would be the CO who was in command during the building of the ship might have a different insight into sensitivities then the CO who is decommissioning a vessel. Consequently, a CO deployed to the 7th Fleet may perceive different threats than a CO who only deployed to the 2nd Fleet.

The next section of the survey sought to determine what is seen as a critical system that has potential sensitivities to a cyber-attack. The major systems of concern

include Combat Systems, Communications, Engineering, Navigation, and Weapons. "Other" has been included in the event that the individual considers another system more sensitive than those listed do. This will help ensure no system is overlooked. The way ahead will be established by addressing the system that is seen as the most sensitive overall. It is imperative to address the most sensitive systems first rather than attempting to secure funding for all systems.

Further determination of sensitive systems requires differentiating between systems that may not be seen as sensitive and those that are. This question is posed the same as the previous, also with the "Other" option to ensure any overlooked systems have an opportunity to be called out and addressed.

Communications systems are critical to the day-to-day mission of the ship. These systems include messaging systems that are of three possible types unclassified (UNCLAS) or non-secure internet protocol router (NIPR), secret (S) or secure internet protocol router (SIPR), and top secret (TS) for joint worldwide intelligence communications system (JWICS). All of these systems allow ships to communicate between each other, aircraft, satellites, and shore facilities. The sensitivity here is that adversaries or cyber terrorists could intercept, monitor, and/or alter communications to and from a ship. The harm in this could be as minimal as email SPAM or as major as altered orders.

Navigation systems are critical for the safe maneuvering of all deployed ships. All ships have charts but also rely on navigational systems (e.g., Furuno radar). An industry standard, it may have the potential to be intercepted and altered by well-informed hackers in the future. An unencrypted, COTS geospatial positioning system (GPS) is a potential liability in ensuring a ship remains on course. If an adversary could harness the technology to manipulate the data, a CO and his/her ship could head off course and be out of range of a supply ship or a port to resupply. In the event that a navigational system is manipulated, ships may be unable to avoid submerged obstructions (e.g., underwater mountains or sunken vessels). Navigation systems are critical to the safety of the ship and crew; if they become compromised, there is the potential for error resulting in either grounding or veering off course.

Engineering systems are also critical to all of the hotel services aboard, (e.g., water and electricity) in addition to allowing a ship to sail. In a time when readings are taken by watchstanders digitally, systems have potentially increased sensitivity to cyber intrusion. If readings can be manipulated, propulsion and engine systems may overheat or run out of oil, causing systems to degrade or to at worst become irreparably damaged. This would cause the ship to be a "sitting duck" susceptible to physical attack.

Attacks on the hotel services and reliance on local port operations and their services would force a ship to return to port to repair the systems or receive almost daily underway replenishments (UNREPs) of food and water. Ships must be replenished at sea or pull into the nearest port before they deplete their fuel onboard. While most sailors could survive a few days without showering or clean clothes and food can be served on paper plates, water is necessary to chill vital computer systems. Having hotel systems inoperable would limit a ship's time between replenishments or pulling into port. Limiting a ship's ability to operate independently would give potential adversaries an advantage. For these reasons it is important consider the potential sensitivity of engineering systems to attack.

"Other" systems could include any of those not covered by the previous discussion. COs afloat that have had ships equipped with weather systems may feel them to be the most important. A degraded weather system may cause a ship to steer into heavy seas. An adversary could potentially influence an entire carrier strike group (CSG) to sail into rough weather leaving them sensitive to attack and limiting their ability to conduct sustained flight operations. Another sensitive area could be those systems used in flight operations. The manipulation of these may leave a helicopter detachment or entire airwing grounded. These are two examples of possible "other" systems that may be seen as sensitive to COs.

# IV. ANALYSIS OF DATA

In-depth data was gathered from surveys of current and past COs in conjunction with existing data from previous studies. Those polled included officers that held command at LT—two, LCDR—three, CDR—eight, and CAPT—three (see Table 1). The platforms represented by this group included MCM—one, PC—one, FFG—seven, DDG—three, and CG—two (see Table 2). This allowed for insight beyond the cruiser and destroyer (CRUDES) community. With the background of those surveyed including various platform experiences, experiences on these platforms as CO were collated with their experiences on other platforms in capacities other than COs. This was highlighted in later questions where responders discussed both LCSs and CVNs. There was a lack of amphibious experience, so this work may not prove applicable to the transportation of Marines to various areas of operations (AORs) as well as their C4I construct while en route.

| LT | LCDR | CDR | CAPT |
|---|---|---|---|
| XX | XXX | XXXXXXXX | XXX |

Table 1. Rank at time(s) of command afloat.

| MCM | PC | FFG | DDG | CG |
|---|---|---|---|---|
| X | X | XXXXXXX | XXX | XX |

Table 2. Platform commanded afloat.

Seven of those surveyed had served in the WEPS or combat systems officer (CSO) role prior to command; this allowed an appreciation of the Navy's weapons and communications suites, as well as potential sensitivities to these. None of the participants had BMD experience; this may have provided insight into a growing area with the forward deployment of four BMD-capable DDGs to 6th Fleet. The majority of those who responded had only one command-at-sea tour (see Table 3).

| One | Two | Three | Four or More |
|---|---|---|---|
| XXXXXX | XX | X | X |

Table 3. Number of At Sea Commands.

The next section of questions focused on ship-specific concerns (i.e., a comparison of the various platforms to see if one was seen as more susceptible to cyber-attack than the others were). First, they were asked to rank a ship's sensitivity to cyber related attacks with 1 being least sensitive and 5 being most sensitive (see Table 4). Then in order to clarify their reasoning, they were asked which platform was most sensitive and which platform was least sensitive. Three responses were that all Navy ships are equally sensitive, CG/DDG/FFG/LCS each received two votes for most sensitive, and CVN received one vote.

| | 1 (least) | 2 | 3 | 4 | 5 (most) |
|---|---|---|---|---|---|
| **CVN** | | | | X | X |
| **Amphib** | | X | XX | XX | XX |
| **CG** | | | X | XXXXX | XXXX |
| **DDG** | | | XXX | XXX | XXX |
| **FFG** | X | XX | X | X | XXXX |
| **LCS** | X | X | X | | XX |
| **MCM** | | X | X | | X |
| **PC** | | | X | | XX |

Table 4. Ships ranked by sensitivity to cyber related attacks.

For least sensitive, four responses stated that all Navy ships were sensitive to an extent. Five responses focused on the smaller platforms (i.e., FFGs/LCSs/MCMs/PCs). In addition, one respondent felt CVNs were the least sensitive. For FFGs, their limited use

due to pending decommissioning makes the employment of a program like the CAD system unlikely to be worth the cost. Cooperation Afloat Readiness And Training (CARAT) missions are their main tasking. These are usually UNCLAS in nature and use limited weapons systems making it unlikely that an adversary may gain anything. LCSs are relatively new and have yet to be incorporated into the CSG framework. They therefore do not currently appear to pose any benefit to the enemy if compromised. MCMs and PCs also are not incorporated in the CSG framework, and do not currently have a critical role in the C4I network of a CSG. Asked to rank these four small ship types against CVNs, amphibious ships, CGs, and DDGs, one can see why they ranked so low. The outlier was the respondent that felt CVNs were the least sensitive. This may be seen as their lack of weapons and combat systems; however, it would not account for the attached carrier air wing (CAW).

The next section was on cyber threats. The purpose here was to gauge whether the individual sees cyber as a potential weapon to be used by an adversary (see Table 5), seven viewed it as a threat. Of the three that did not, two were retired post major command (i.e., prior to the advent of cyber being a critical part of the Navy's C4I construct). The remaining one was in command of an MCM at the time of the survey, and did feel that their ship would be a potential target due to its limited assets and specific mission. With those three exceptions, the remaining seven viewed it as an actual threat to the CG/DDG/FFG they were in command of. This essentially validates the need to address concerns of COs at sea in order to protect potentially sensitive assets.

| | **Yes** | **No** |
|---|---|---|
| **Is cyber terrorism a threat?** | XXXXXXX | XXX |

Table 5. Cyber terrorism, currently a threat or not to ships.

Next, the respondents were asked to highlight when they felt a ship would be most and least sensitive to a cyber-attack (see Table 6). Half responded that a ship is always sensitive, three said while in homeport, and two said when deployed. The

majority viewing it as a threat always again highlights the need to address concerns of those COs in command. Those viewing homeport could be due to the network being established and potentially infiltrated over time. The two claiming on deployment may be due to potential threats while using wireless fidelity (WIFI) or internet connections in foreign ports. Alternatively, they may have been alluding to the adversary being able to reach out to our networks by other means while deployed (e.g., previously compromised hardware or software).

For the time when a ship would be least sensitive to a cyber-threat (see Table 6), five saw this as an unlikely scenario as long as systems were powered on and connected. Two felt during fleet level exercises, two felt during deployments, and one in homeport. The reasoning provided for it being during exercises (e.g., Independent Deployer Certification Exercise [IDCERTEX] or COMPTUEX) is that ships would be expecting to be attacked by opposing forces. They would therefore be extra vigilant in their defense of shipboard networks. If a non-exercise player attempted to gain access, there would be a higher likelihood of that action being exposed. Those two responding while on deployment, raised the point that, at least currently, it is difficult to compromise a unit at sea given they are not hardwired to a network. In addition, the lone respondent that stated while in homeport may have felt that a ship tied up to a pier would not be appealing to a cyber-terrorist.

| | **Always** | **Homeport** | **Exercises** | **Deployment** | **Never** |
|---|---|---|---|---|---|
| **Most Vulnerable** | XXXXX | XXX | - | XX | - |
| **Least Vulnerable** | - | X | XX | XX | XXXXX |

Table 6. Periods of sensitivity to cyber-attacks.

WIFI is a part of everyday life and can be used to make individuals more mobile in terms of shipboard work. The crew uses wireless technology aboard ships to share movies, games, etc. While this technology is not connected to shipboard networks or to

off ship internet protocol (IP) services, it may in the future. The respondents were five for, four against, and one not applicable (N/A) as to whether ships should be able to use WIFI while in port (see Table 7). Benefits would include increased morale for crews as well as the ability for technicians to troubleshoot on scene while coordinating with distance support. Over the course of a year, the time spent tethered to a desktop or laptop connected to the network adds up. With technology available to allow sailors to be connected while walking throughout a ship or while working in a space, it should not be discounted due to potential cyber threats. Rather it should be a guarded network that allows sailors to increase productivity.

| | For | Against | N/A |
|---|---|---|---|
| **WIFI In Port** | XXXXX | XXXX | X |

Table 7. Position on WIFI for ships in port.

The next section dealt with cyber protection and implementation necessity (see Table 8). The point of this section was to have those surveyed draw upon past and current experiences in determining when a program like the CAD system should be installed. When the Navy implements a new system, there are several different ways of rolling it out to the fleet. They could do it by ship type (e.g., Remote Mine Submersible [RMS] was installed on Flight IIA DDGs). Another method would be to do so based on Numbered Fleet (e.g., a specific Fleet's ships could get a modification to a system based on a perceived threat in that region). Prior to deployment, ships have continuous maintenance availabilities (CMAVs). During this time, ships could be outfitted with a new system to take forward into theater. Another two options may include either during initial construction or during mid-life upgrade.

The majority of respondents, eight out of 10, leaned towards a system to help combat cyber threats (e.g., the CAD system) being installed during the initial construction. If the technology is available and approved for shipboard use that would allow a CO at sea to better defend their ship, it should be made available during initial construction. This allows a crew to be accustomed to working with a system rather than

the alternative of being unprotected and having to learn a new system later in the ship's life.

The second most favored approach was during the mid-life upgrade of the ship. During this period, multiple systems of a ship are removed, replaced, or upgrade. It would allow new technologies not available at initial construction to be incorporated into the C4I structure of defending a ship. This allows technology to be installed that will counter threats that were not present 15, 20, even 25 years prior.

The majority did not view the other three options (pre-deployment, by numbered Fleet, and by ship type) as preferred options. Reasons for this are addressed earlier in the survey where the majority saw cyber threats as real and could affect all navy ships. If the enemy can reach a Seventh Fleet asset, they could just as easily infiltrate a Third Fleet asset. For a platform specific approach, those surveyed favored addressing CRUDES platforms, but the responses to this question highlight the desire to install technology across all platforms. Finally, pre-deployment seemed to either be too late and to be an added hurdle prior to deployment.

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| **By Ship Type** | XX | - | XXXX | - | XX |
| **By Numbered Fleet** | - | XX | XXX | XX | X |
| **Pre-Deployment** | X | X | XX | XXXX | X |
| **Mid-life Upgrade** | - | X | XXX | XX | XXX |
| **Initial Construction** | X | - | - | - | XXXXXXXX |

Table 8. How/when to implement a cyber-protection system on a ship.

The next section addressed fiscal concerns given the increased need to be fiscally responsible in recent years (see Table 9). The survey asked participants to rank the areas where cyber could be addressed: offensive, training, maintenance, defensive, guidance, and other. These five areas along with others allow for a discussion on determining what

source of funding may best be used to protect ships against cyber. Offensive measures would be employing technology that would protect against cyber-attacks. Training encompasses such means as General Military Training (GMT), lessons on Navy Knowledge Online (NKO), or at schoolhouses across the Fleet. Maintenance would be used to improve the current cyber protection infrastructure (e.g., protecting existing shipboard networks by upgrading hardware and software). Defensive would be to install cyber protection systems or processes (e.g., the CAD system). Guidance includes cyber implementation and protection policy. Other was provided for the respondents in the event they thought of another way to address the issue through funding.

The two means receiving the lowest support were offensive measures and guidance. The latter of these two may have seemed as taking too long or being ineffective in the end. With cyber threats, it is critical to address them as they arise rather than attempt cultural or institutional change, which tends to take months or years to spread across an organization. Investing limited funds and resources on rhetoric would leave shipboard networks sensitive for the short-term and potentially longer.

Cyber training received feedback that is more positive. Instituting training (e.g., the annual IA training mandatory for all personnel using Navy networks) ensures a baseline level of knowledge throughout the Fleet. Required training for seaman recruits through ADMs has the potential to, at a minimum; make all sailors aware of the threats facing all ships and naval assets. This approach addresses awareness and ways to use systems more securely. However, it does not address an adversaries' ability to access shipboard networks.

The approach receiving the second most consideration was maintenance. This would address existing flaws and weaknesses in current shipboard networks. Rather than replacing everything and starting over, those surveyed find shoring up existing cyber infrastructure as a viable option. This could include repairing cabling, switches, routers, etc. Another important avenue is to ensure that antivirus software is up-to-date on all networks (NIPR, SIPR, JWICS, etc.). Existing shipboard networks should be maintained at their highest state of readiness due to the Navy's increased reliance on such venues as chat for keeping Fleet Commanders apprised of the disposition of their forces afloat. If a

unit is independently deployed and their shipboard network is compromised, they may be unable to maintain communications with the local sea combat commander.

The overwhelming response was for a defensive approach to protecting shipboard networks (e.g., the CAD system). The installation of a new system to protect a ship better appears to be the favored approach for many reasons. One would be due to the time in which it can be accomplished. A phased approach to installation could be completed utilizing CMAV or specialized-repair activity (SRA).

| | 1 (lowest) | 2 | 3 | 4 | 5 (highest) |
|---|---|---|---|---|---|
| **Offensive** | XX | XX | XXXX | X | X |
| **Training** | X | X | X | XX | XXXX |
| **Maintenance** | - | X | XX | XX | XXXXX |
| **Defensive** | - | - | XX | XX | XXXXXX |
| **Guidance** | X | XXXXXX | X | XX | X |
| **Other: Homefront Hacking** | - | - | - | - | X* |

Table 9. Prioritization of means of cyber protection given focus on fiscal constraint.

The next section of the survey attempted to determine if any particular department on a ship was more or less sensitive to cyber intrusions (see Table 10). In an attempt to identify a department or departments, respondents ranked combat systems, operations, engineering, administrative, weapons, and other from least sensitive to most sensitive to such a threat. 'Other' allowed for a department that may have been overlooked to be identified.

Half of the respondents viewed the Combat Systems Department (and its Communications Division) and Operations as the most sensitive. This seems to be the

most logical due to the importance of a ship at sea being able to not only communicate with higher headquarters but also being able to utilize its combat systems suite to defend itself. Communication is critical within CSGs, amphibious readiness groups, and surface action groups. This illuminates an area of concern in regard to a need for improved/maintained cyber protection.

As far as least sensitive, half of respondents saw Engineering Department as the least sensitive to cyber terrorists. One of the reasons behind this may be the fact that the majority of Engineering Department's systems are standalone and confined to the ship and do not require access to a penetrable ship to ship or ship to shore interface. The exceptions would be reports that are sent off ship about fuel amounts or maintenance concerns. The remaining respondents were split between Weapons, Supply, and Admin Departments.

| | 1 (least) | 2 | 3 | 4 | 5 (most) |
|---|---|---|---|---|---|
| **Combat Systems** | X | - | XX | XX | XXXXX |
| **Operations** | - | X | - | XXX | XXXXX |
| **Engineering** | XXX | - | XX | XXX | X |
| **Administrative** | XXX | XX | - | XX | XX |
| **Weapons** | X | XX | XX | XX | XX |
| **Other: Supply** | - | - | - | - | X |

Table 10. Departments' sensitivity to cyber-attack.

In an effort to find if there was a common person in charge across the Fleet, respondents were asked who is currently in charge of cyber threats. Three respondents have seen it be a chief petty officer, two have seen it be a DH, one each had seen it be a DIVO, an IT1, C10F, unsure, and in once instance a combination of CO and another officer. This highlights a varied approach across commands, and the potential for a single

position being identified for commonality fleet wide. To see the level of importance placed on this area they were asked how these individuals were appointed: as either their primary duty, collateral duty, or another means. Six had seen it be the collateral duty and three had seen it be the primary duty. The trend of it being a collateral duty rather than a primary duty

The next follow on questions asked which department should be in charge of cyber (see Table 11) and whether or not they should have a counterpart on staff. Four saw this falling under combat systems purview, three saw it as an operations area, and one felt communications as a department should oversee it, one felt either combat systems or operations, and one was undecided. The majority see it as a Combat Systems Department area of responsibility, particularly Communications Division, also known as CC (Combat Systems-Communication) Division others seeing it as an operations department area could be given the potential for Communications Division to be a part of Operations Department as OC (Operations-Communication) Division. All but one respondent saw the need for a counterpart on staff that could address concerns of a ship as well as represent the collective concerns of a destroyer squadron (DESRON) or CSG.

| | **Combat Systems** | **Operations** | **Communications** | **Undecided** |
|---|---|---|---|---|
| **Cyber Division** | XXXXX | XXXX | X | X |

Table 11. Department that a Cyber Division should report to.

In order to see what level of training may be needed to prepare unrestricted line (URL) officers for command, they were asked at what level it should be given (see Table 12). The options were DIVO training, currently Basic Division Officer Course (BDOC), DH school, or during the XO/CO pipeline. The majority of respondents fell that it was necessary to have training at every level. In one instance, it was not seen as necessary for DHs, and another instance seen as not necessary for DIVOs. Two surveyed felt it was enough to have it at the DIVO level. The majority highlights COs afloat seeing a need for

cyber training at all levels. The one reply that did not list DH may be given the amount of information currently covered at SWOS in six months for an individual prior to two 18-month tours that may or may not involve direct interaction with Combat Systems Department or communications division. However, when reflected in Table 12 there is a clear trend for a cyber-threats and cyber protections to be taught at all levels to URL officers.

| | BDOC | DH | XO/CO |
|---|---|---|---|
| **Training Pipeline** | XXXXXXXXX | XXXXXXX | XXXXXXXX |

Table 12. Preferred training pipeline to teach cyber.

Finally, the last question involved the ranking of methods to prepare sailors for dealing with cyber threats (see Table 13). The categories were all-hands training, early warning detection systems, outsourcing systems and maintenance, schooling for operators, the use of COTS systems, the CAD system, simulators, or some other method. The overwhelming number of respondents favored schooling for operators. This would allow a CO to have Sailors trained to detect and defend against cyber threats. The next most favored approach was the CAD system. The least favored approach would be to outsource systems and their maintenance. This was expected due to the potential for compromise of critical systems. One respondent replied data visualization.

| | 1 (least) | 2 | 3 | 4 | 5 (most) |
|---|---|---|---|---|---|
| **All Hands Training** | XXX | - | XX | - | XXXX |
| **Early Warning System** | - | X | XXX | X | XXX |
| **Outsourcing** | XXX | XXXX | X | - | - |
| **Schools** | - | - | XX | XXX | XXXX |

| | 1 (least) | 2 | 3 | 4 | 5 (most) |
|---|---|---|---|---|---|
| **COTS** | - | XX | X | XXX | X |
| **CADS** | - | - | XX | XXXX | XX |
| **Simulators** | X | X | XXX | XX | X |
| **Other: Data Visualization** | - | - | - | - | X |

Table 13. Preferred methods for preparing sailors for cyber threats.

# V. CONCLUSIONS AND RECOMMENDATIONS

The data provides relatively clear indication regarding the following issues as perceived by the COs polled. First, cyber-threats are real and pose a real threat to naval warships afloat. Current and former COs see cyber-threats as a current concern not a problem still 10-15 years out. Second, combat systems departments onboard ships are at the greatest risk for cyber intrusion due to overseeing all communications on and off ship. Radio transmissions are required to able to travel from higher headquarters to the warship that is forward deployed. If these transmissions are delayed or intercepted, a CO may never receive the reinforcement they require or may not reach the battle they were headed to participate in. Third, the CAD system appears to be seen as viable the COs surveyed as cyber self-defense mechanism.

There is some indication that some COs see operations department as similarly if not more vulnerable to cyber intrusion than combat systems department. Some COs are still unsure of how best to provide WIFI to sailors in port without jeopardizing their shipboard networks. This may be due to a concern for electronic spillage to occur between secure and unsecure networks. While some saw all ships as vulnerable, the CRUDES ships were the ones focused on in particular. FFGs was seen as not being as susceptible to cyber-attack potentially due to their upcoming fleet wide decommissioning. Additionally, there was somewhat of lack of agreeance on who onboard a ship should oversee cyber related issues. Experiences ranged from seeing a first class petty officer all the way through the CO.

The results of the surveys gave little indication of a current system or training mechanism in place that protects ships from sophisticated cyber-attacks. Those surveyed answered based on their experiences; there concerns are those of the warfighter and not the information professional in charge of improving cyber vulnerabilities. However, this did give a prospective that will allow further research to look at other avenues for defending a ship at sea.

Future research should look at the naval processes from a larger scale (e.g., supply routes to sailors on deployment). As one respondent stated, "We must look holistically at the threat and the systems. I can degrade mission success in multiple ways; we seldom look at vectors of attack in a holistic way."[55] There are multiple ways to look at cyber weaknesses of ships at sea. This survey gathered insight from those who have commanded at sea. There is information to be gathered from the DHs, DIVOs, chiefs, and junior sailors that are more technologically advanced that could add to the ongoing discussion. The protection of ships by the CAD system or something similar has merit, and it seems to be inevitable in the further defense our ships and crews that are deployed.

[55] Respondent D, CG CO.

# APPENDIX A. INITIAL SURVEY FROM WINTER 2012

**PLEASE BE ADVISED: DO PUT ANY PERSONALLY IDENTIFIABLE INFORMATION (PII) WITHIN THE SURVEY**

NAVAL POSTGRADUATE SCHOOL, MONTEREY, CA

## Tactics for Protecting Shipboard IT Networks

### A Survey of Current & Former U.S. Navy Commanding Officers (Afloat)

**LT Steven Zielechowski**

**Winter 2012**

The attached survey will help to determine what Commanding Officers Afloat see as the way ahead in protecting US Navy ships from current and potential future cyber threats. The survey builds on two previous NPS theses: (1) Adderson, O. G. and K. A. Wood (2010). *A Qualitative Analysis of Strategic Capabilities for a Covert Analysis Detection System Onboard an AEGIS Class Ship* & (2) Crisp, J., L. Hoffman, and M. Schaefer (2010). *Validating the Deployment of a Covert Analysis and Detection System: A Risk Analysis of the Cyber Vulnerabilities and Threats to the Aegis Combat System*. Adderson defined a CAD system as, "a sensor or sensor system that can covertly capture incoming and outgoing data while analyzing and maintaining control of the data." And stated, "The use of a CAD system may help to increase the overall awareness about attackers while sustaining peak levels of combat readiness through remaining discrete while protecting our own information systems."

It has been suggested that the Navy consider deploying a CAD system in the Aegis Combat System in order to better secure the system against potential cyber intrusions or attacks. This system will be designed to covertly detect intrusions of malicious programs and to track their activities and behavior. These data will only be available to the CO and designated shipboard personnel. It may be possible for CADS to deceive the malicious software and/or isolate it to keep it from causing harm.

When taking the survey, please draw from your personal experience as a Commanding Officer Afloat. The overall goal is to determine if the CAD system or something similar is a valid approach to protect afloat systems from Cyber attack or Cyber intrusion by unfriendly countries or terrorists.

If you need clarification on a question or need further definition of any terms, do not hesitate to contact me at either szielech@nps.edu or (724) 812-3870.

Do you mind being contacted for clarification regarding your answers on this survey?

☐Yes, please do not contact me ☐No, feel free to contact me

Contact Information:

Name:_____

Phone:_____

E-mail:_____

Very Respectfully,

LT Steven Zielechowski

**PLEASE BE ADVISED: DO PUT ANY PERSONALLY IDENTIFIABLE INFORMATION (PII) WITHIN THE SURVEY**

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

# Tactics for Protecting Shipboard IT Networks

***Purpose***: Data gathered here will be used to build upon previous NPS theses that presented Covert Analysis Detection (CAD) System as a viable option for the defense of ships from cyber attacks.

### *General Information*

1. Rank at time of At-Sea Command (check all that apply):
   - ☐ Lieutenant (LT)
   - ☐ Lieutenant Commander (LCDR)
   - ☐ Commander (CDR)
   - ☐ Captain (CAPT)

2. Type of ship (check all that apply):
   - ☐ Amphibious Ship, type _____
   - ☐ Cruiser (CG)
   - ☐ Destroyer (DDG)
   - ☐ Frigate (FFG)
   - ☐ Littoral Combat Ship (LCS)
   - ☐ Other, type _____

3. Weapons Department / Combat Systems Department experience:
   - ☐ Yes
   - ☐ No

4. Were any ships BMD capable?
   - ☐ Yes
   - ☐ No

5. Number of At-Sea Commands:
   - ☐ None
   - ☐ One
   - ☐ Two
   - ☐ Three
   - ☐ Four or more

### *Ship Specific Concerns*

6. Rank each ship's vulnerability to cyber related attacks (1—least, 5—most):

| | | | | | |
|---|---|---|---|---|---|
| Amphibious Ship, type _____ | 1 | 2 | 3 | 4 | 5 |
| Cruiser (CG) | 1 | 2 | 3 | 4 | 5 |
| Destroyer (DDG) | 1 | 2 | 3 | 4 | 5 |
| Frigate (FFG) | 1 | 2 | 3 | 4 | 5 |
| Littoral Combat Ship (LCS) | 1 | 2 | 3 | 4 | 5 |
| Other, type _____ | 1 | 2 | 3 | 4 | 5 |

7. Which ship type is currently most vulnerable to cyber attack?
   - ☐ Amphibious Ship, type _____
   - ☐ Cruiser (CG)
   - ☐ Destroyer (DDG)
   - ☐ Frigate (FFG)
   - ☐ Littoral Combat Ship (LCS)
   - ☐ Other, type _____
   - ☐ No Difference

8. Which ship type is currently least vulnerable to cyber attack?
   - ☐ Amphibious Ship, type _____
   - ☐ Cruiser (CG)
   - ☐ Destroyer (DDG)
   - ☐ Frigate (FFG)
   - ☐ Littoral Combat Ship (LCS)
   - ☐ Other, type _____
   - ☐ No Difference

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

Additional Comments on Ship Specific Concerns:

_____

_____

_____

***Cyber Threats***

9. While in Command, did you view cyber terrorism as a threat?
   - ☐ Yes
   - ☐ No
10. Do you view cyber terrorism as a threat?
    - ☐ Currently (within next 10 years)
    - ☐ In the future (over 10 years away)
11. When is a ship most vulnerable?
    - ☐ Homeport
    - ☐ Port Visits
    - ☐ Deployment
    - ☐ Exercises
    - ☐ Other: _____
12. When is a ship least vulnerable?
    - ☐ Homeport
    - ☐ Port Visits
    - ☐ Deployment
    - ☐ Exercises
    - Other: _____
13. Should ships refrain from Wi-Fi use while in port to avoid potential cyber attacks?
    - ☐ Yes
    - ☐ No

Additional Comments on Cyber Threats:

_____

_____

_____

***Cyber Protection Implementation & Necessity***

14. Given the potential for cyber attack, rank each method of implementing a cyber protection program/system (e.g., Covert Analysis Detection (CAD) System[1]), would be effective (1—least, 5—most):

| | | | | | |
|---|---|---|---|---|---|
| By Ship Type | 1 | 2 | 3 | 4 | 5 |
| By Numbered Fleet | 1 | 2 | 3 | 4 | 5 |
| Pre Deployment Pacakge | 1 | 2 | 3 | 4 | 5 |
| During Mid-life Upgrade | 1 | 2 | 3 | 4 | 5 |
| During Intial Building | 1 | 2 | 3 | 4 | 5 |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Cyber Protection Implementation & Necessity:

_____

_____

[1] "A CAD (Covert Analysis Detection) system is a sensor or sensor system that can covertly capture incoming and outgoing data while analyzing and maintaining control of the data." —Adderson, O. G. and K. A. Wood. (2010). *A Qualitative Analysis of Strategic Capabilities for a Covert Analysis Detection System Onboard an AEGIS Class Ship*. Monterey, Calif.: Naval Postgraduate School.

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

***Fiscal Concerns***

15. Given fiscal constraints, it is necessary to prioritize process/system implementation, upgrade, and training. Prioritize the below areas in regards to Cyber protection of ships (1—lowest priority, 5—highest priority):

| | | | | | |
|---|---|---|---|---|---|
| Offensive, e.g., Protecting against Cyber Attacks | 1 | 2 | 3 | 4 | 5 |
| Training, e.g., Cyber | 1 | 2 | 3 | 4 | 5 |
| Maintenance, e.g., Cyber Protection Infrastructure | 1 | 2 | 3 | 4 | 5 |
| Defensive, e.g., Install Cyber Protection Systems/Processes | 1 | 2 | 3 | 4 | 5 |
| Guidance, e.g., Cyber Implementation/Protection Policy | 1 | 2 | 3 | 4 | 5 |
| Other Areas of Cyber Concern: _____ | 1 | 2 | 3 | 4 | 5 |

16. Rank the below methods of implementation to increase cyber protection through systems/processes:

| | | | | | |
|---|---|---|---|---|---|
| Fleetwide | 1 | 2 | 3 | 4 | 5 |
| Deployed Platforms Only | 1 | 2 | 3 | 4 | 5 |
| Only When a Threat is Deemed Imminent | 1 | 2 | 3 | 4 | 5 |
| Platform Specific (which: _____) | 1 | 2 | 3 | 4 | 5 |
| Other Method: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Fiscal Concerns:

***Shipboard Network Concerns***

17. Which system is most vulnerable to cyber attack or cyber intrusion?
- ☐ Combat Systems
- ☐ Communications
- ☐ Engineering
- ☐ Navigation
- ☐ Weapons
- ☐ Other: _____

18. Which system is least vulnerable to cyber attack or cyber intrusion?
- ☐ Combat Systems
- ☐ Communications
- ☐ Engineering
- ☐ Navigation
- ☐ Weapons
- ☐ Other: _____

19. Who is usually designated to be in charge of Cyber Threat?
- ☐ Department Head
- ☐ Division Officer
- ☐ CPO
- ☐ Other: _____

20. How is this person designated?
- ☐ Primary Duty
- ☐ Collateral Duty
- ☐ Other: _____

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

21. Cyber threats can potentially affect each Department to varying degrees, rank each Department's sensitivity to such a threat (1—least, 5—most):

| | | | | | |
|---|---|---|---|---|---|
| Combat Systems | 1 | 2 | 3 | 4 | 5 |
| Operations | 1 | 2 | 3 | 4 | 5 |
| Engineering | 1 | 2 | 3 | 4 | 5 |
| Administrative | 1 | 2 | 3 | 4 | 5 |
| Weapons | 1 | 2 | 3 | 4 | 5 |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

22. Which Department should oversee Cyber protection and policy?
- ☐ Combat Systems
- ☐ Operations
- ☐ Engineering
- ☐ Administrative
- ☐ Weapons
- ☐ Other: _____

23. Should the Department in charge of Cyber have a counterpart on Staff?
- ☐ Yes
- ☐ No

24. Should increased Cyber Training be given to unrestricted line (URL) Officers?
- ☐ Yes
- ☐ No

25. If yes, when should Cyber Training be given (check all that apply)?
- ☐ SWOS
- ☐ DH School
- ☐ XO/CO School
- ☐ Other: _____

Additional Comments on Shipboard Network Concerns:

_____

_____

_____

***Further Addressing Shipboard Network Concerns***

1. Rank each methods potential to help better prepare shipboard personnel for dealing with potential cyber threats (1—lowest, 5—highest):

| | | | | | |
|---|---|---|---|---|---|
| All Hands Training | 1 | 2 | 3 | 4 | 5 |
| Early Warning Detection Systems, type _____ | 1 | 2 | 3 | 4 | 5 |
| Outsourcing Systems and Maintenance | 1 | 2 | 3 | 4 | 5 |
| Schooling for Operators | 1 | 2 | 3 | 4 | 5 |
| Use of COTS | 1 | 2 | 3 | 4 | 5 |
| Covert Analysis Detection System (CADS) | 1 | 2 | 3 | 4 | 5 |
| Simulators | 1 | 2 | 3 | 4 | 5 |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

Additional Comments on Further Addressing Shipboard Network Concerns:

_____

_____

_____

***Additional Information***

Additional Comments / Suggestions:

_____

_____

_____

_____

When you are done, please e-mail the survey back to me at szielech@nps.edu.

***Thank you for your participation!***

# APPENDIX B. UPDATED SURVEY FROM WINTER 2013

PLEASE BE ADVISED: DO NOT PUT ANY PERSONALLY IDENTIFIABLE INFORMATION (PII) WITHIN THE SURVEY

NAVAL POSTGRADUATE SCHOOL, MONTEREY, CA

## Tactics for Protecting Shipboard IT Networks

### A Survey of Current & Former U.S. Navy Commanding Officers (Afloat)

LT Steven Zielechowski

Winter 2013

**Survey Purpose:** To gather the perspectives and insights of Commanding Officers Afloat, both current and former. The purpose is not to provide definitive answers to the questions presented.

When taking the survey, please draw from your personal experience as a Commanding Officer Afloat. The overall goal is to determine if the Covert Analysis Detection (CAD) system, which is described on the next page, is a valid approach to protect afloat systems from Cyber attack or Cyber intrusion by unfriendly countries or terrorists.

If you need clarification on a question or need further definition of any terms, do not hesitate to contact me at either szielech@nps.edu or (724) 812-3870.

Do you mind being contacted for clarification regarding your answers on this survey?

□Yes, please do not contact me □No, feel free to contact me

Contact Information:

Name:_____

Phone:_____

E-mail:_____

PLEASE BE ADVISED: DO NOT PUT ANY PERSONALLY IDENTIFIABLE INFORMATION (PII) WITHIN THE SURVEY

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

***Covert Analysis Detection (CAD) System Description***

The Covert Analysis Detection (CAD) system concept has been looked at by the Program Executive Office Integrated Warfare Systems (PEO IWS) as well as in student thesis work. Previous NPS theses include: Adderson, O. G. and K. A. Wood (2010). *A Qualitative Analysis of Strategic Capabilities for a Covert Analysis Detection System Onboard an AEGIS Class Ship* & Crisp, J., L. Hoffman, and M. Schaefer (2010). *Validating the Deployment of a Covert Analysis and Detection System: A Risk Analysis of the Cyber Vulnerabilities and Threats to the Aegis Combat System*. Adderson defined a CAD system as, "a sensor or sensor system that can covertly capture incoming and outgoing data while analyzing and maintaining control of the data." And stated, "The use of a CAD system may help to increase the overall awareness about attackers while sustaining peak levels of combat readiness through remaining discrete while protecting our own information systems."

This survey was designed to identify the need or lack of need for an active defense system afloat, e.g., the CAD system, to protect shipboard networks from possible cyber attacks. As hacking methods evolve, it is likely that nation-states and terrorists will attempt to interfere with or take control of shipboard systems remotely. The previously mentioned theses suggest that the Navy consider deploying a CAD system in the Aegis Combat System better secure the system against potential cyber intrusions or attacks. This system could covertly detect intrusions of malicious programs and track their activities and behavior, deceive the malicious software, and/or isolate it to keep it from causing irreparable harm. The data would only be available to the CO and designated shipboard personnel.

An example of the CAD system: A CO using the CAD system that has just received an intelligence report that an adversary may have infiltrated and have access into the Aegis system aboard their ship would be able to make decisions that include but are not limited to:

1) Allowing the adversary to believe they have control of the Aegis system, when they in fact do not. This can be described as a "honey pot," where the adversary believes they have infiltrated a system but in reality it is just a decoy and their actions are being monitored to improve cyber defenses.
2) Provide misleading information to the adversary regarding systems status, e.g., the system appears to be non-operational when it is not or vice versa.
3) Disrupt but not disconnect the adversary's access into the system to create confusion or delay that allows for their identity or capabilities to become known.
4) Disconnecting the adversary from the identified access path that they used to infiltrate the Aegis system.

The results of this survey will be used to encourage or discourage further research into Cyber protection for shipboard networks. The final data will be used as a baseline for the determination of the need to install a system like CAD to provide COs with an extra layer of protection from potential Cyber attacks. Future surveys may be conducted amongst Department Heads, Senior Operators, et al to further define the need for Cyber protection through processes and systems for shipboard networks.

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

# Tactics for Protecting Shipboard IT Networks

***Purpose***: Data gathered here will be used to build upon previous NPS theses that presented Covert Analysis Detection (CAD) System as a viable option for the defense of ships from cyber attacks.

### *General Information*

1. Rank(s) at time of At-Sea Command (check all that apply):
   - ☐ Lieutenant (LT)
   - ☐ Lieutenant Commander (LCDR)
   - ☐ Commander (CDR)
   - ☐ Captain (CAPT)
2. Number of At-Sea Commands:
   - ☐ None
   - ☐ One
   - ☐ Two
   - ☐ Three
   - ☐ Four or more
3. Were you ever a Weapons or a Combat Systems Department Head?
   - ☐ Yes
   - ☐ No
4. Were any of your ships Ballistic Missile Defense (BMD) capable?
   - ☐ Yes
   - ☐ No
5. Type of ship(s) (check all that apply):
   - ☐ Aircraft Carrier (CVN)
   - ☐ Amphibious Ship (LHA/LHD, LCC, LPD, or LSD), type _____
   - ☐ Cruiser (CG)
   - ☐ Destroyer (DDG)
   - ☐ Frigate (FFG)
   - ☐ Littoral Combat Ship (LCS)
   - ☐ Mine Countermeasures Ship (MCM)
   - ☐ Patrol Coastal Ship (PC)
   - ☐ Other, type _____

### *Ship Specific Concerns*

6. Individually rate each ships' overall vulnerability to a cyber related attack (1—lowest, 2—low, 3—average, 4—high, 5—highest):

| | | | | | |
|---|---|---|---|---|---|
| Aircraft Carrier (CVN) | 1 | 2 | 3 | 4 | 5 |
| Amphibious Ship (LHA/LHD, LCC, LPD, or LSD), type _____ | 1 | 2 | 3 | 4 | 5 |
| Cruiser (CG) | 1 | 2 | 3 | 4 | 5 |
| Destroyer (DDG) | 1 | 2 | 3 | 4 | 5 |
| Frigate (FFG) | 1 | 2 | 3 | 4 | 5 |
| Littoral Combat Ship (LCS) | 1 | 2 | 3 | 4 | 5 |
| Mine Countermeasures Ship (MCM) | 1 | 2 | 3 | 4 | 5 |
| Patrol Coastal Ship (PC) | 1 | 2 | 3 | 4 | 5 |
| Other, type _____ | 1 | 2 | 3 | 4 | 5 |

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

7. Overall, which ship type is currently the *most* vulnerable to a cyber attack?
   - ☐ Aircraft Carrier (CVN)
   - ☐ Amphibious Ship (LHA/LHD, LCC, LPD, or LSD), type _____
   - ☐ Cruiser (CG)
   - ☐ Destroyer (DDG)
   - ☐ Frigate (FFG)
   - ☐ Littoral Combat Ship (LCS)
   - ☐ Mine Countermeasures Ship (MCM)
   - ☐ Patrol Coastal Ship (PC)
   - ☐ Other, type _____

8. Overall, which ship type is currently the *least* vulnerable to a cyber attack?
   - ☐ Aircraft Carrier (CVN)
   - ☐ Amphibious Ship (LHA/LHD, LCC, LPD, or LSD), type _____
   - ☐ Cruiser (CG)
   - ☐ Destroyer (DDG)
   - ☐ Frigate (FFG)
   - ☐ Littoral Combat Ship (LCS)
   - ☐ Mine Countermeasures Ship (MCM)
   - ☐ Patrol Coastal Ship (PC)
   - ☐ Other, type _____

Additional Comments on Ship Specific Concerns:

_____

_____

_____

***Cyber Threats***

9. While in Command, did you view cyber terrorism as a threat?
   - ☐ Yes
   - ☐ No

10. Cyber Terrorism is a _____ threat.
    - ☐ Current (within next 10 years)
    - ☐ Future (over 10 years away)

11. When is a ship *most* vulnerable?
    - ☐ Homeport
    - ☐ Port Visits
    - ☐ Deployment
    - ☐ Exercises
    - ☐ Other: _____

12. When is a ship *least* vulnerable?
    - ☐ Homeport
    - ☐ Port Visits
    - ☐ Deployment
    - ☐ Exercises

    Other: _____

13. Should ships refrain from Wi-Fi use while in port to avoid potential cyber attacks?
    - ☐ Yes
    - ☐ No

Additional Comments on Cyber Threats:

_____

_____

_____

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

***Cyber Protection Implementation & Necessity***

14. Given the potential for a cyber attack, rank the effectiveness of each implementation approach for cyber protection programs/systems, e.g., installing Covert Analysis Detection (CAD) System[1], (1—least effective, 2—less effective, 3—effective, 4—more effective, 5—most effective):

| | | | | | |
|---|---|---|---|---|---|
| By Ship Type | 1 | 2 | 3 | 4 | 5 |
| By Numbered Fleet | 1 | 2 | 3 | 4 | 5 |
| Pre-deployment Package | 1 | 2 | 3 | 4 | 5 |
| During Mid-life Upgrade | 1 | 2 | 3 | 4 | 5 |
| During Intial Shipbuilding | 1 | 2 | 3 | 4 | 5 |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Cyber Protection Implementation & Necessity:

_____

_____

_____

***Fiscal Concerns***

15. Given current and expected future fiscal constraints, it is necessary to prioritize the needs of a ship. Rank the below areas of shipboard Cyber protection (1—lowest priority, 2—lower priority, 3—priority, 4—higher priority, 5—highest priority):

| | | | | | |
|---|---|---|---|---|---|
| Defensive, e.g., Install Cyber Protection Systems/Processes | 1 | 2 | 3 | 4 | 5 |
| Guidance, e.g., Cyber Implementation/Protection Policy | 1 | 2 | 3 | 4 | 5 |
| Maintenance, e.g., Cyber Protection Infrastructure | 1 | 2 | 3 | 4 | 5 |
| Offensive, e.g., Protecting against Cyber Attacks | 1 | 2 | 3 | 4 | 5 |
| Training, e.g., Cyber | 1 | 2 | 3 | 4 | 5 |
| Other Areas of Cyber Concern: _____ | 1 | 2 | 3 | 4 | 5 |

[1] "A CAD (Covert Analysis Detection) system is a sensor or sensor system that can covertly capture incoming and outgoing data while analyzing and maintaining control of the data." —Adderson, O. G. and K. A. Wood. (2010). *A Qualitative Analysis of Strategic Capabilities for a Covert Analysis Detection System Onboard an AEGIS Class Ship*. Monterey, Calif.: Naval Postgraduate School.

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

16. Given current and expected future fiscal constraints, rank the below approaches to the implementation of processes/systems to increase cyber security on ships (1—worst approach, 2—worse approach, 3—acceptable approach, 4—better approach, 5—best approach):

| | | | | | |
|---|---|---|---|---|---|
| Fleetwide | 1 | 2 | 3 | 4 | 5 |
| Deployed Platforms Only | 1 | 2 | 3 | 4 | 5 |
| Only When a Threat is Deemed Imminent | 1 | 2 | 3 | 4 | 5 |
| Platform Specific (which: _____) | 1 | 2 | 3 | 4 | 5 |
| During Initial Shipbuilding | 1 | 2 | 3 | 4 | 5 |
| Other Method: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Fiscal Concerns:

_____

_____

_____

***Shipboard Network Concerns***

17. Which shipboard system is *most critical* during a time of conflict, i.e., must remain online throughout to defend the ship or other assets in the AOR?
    - ☐ Combat Systems
    - ☐ Communications
    - ☐ Engineering
    - ☐ Navigation
    - ☐ Weapons
    - ☐ Other: _____

18. Which shipboard system is *least critical* during a time of conflict?
    - ☐ Combat Systems
    - ☐ Communications
    - ☐ Engineering
    - ☐ Navigation
    - ☐ Weapons
    - ☐ Other: _____

19. Who is usually designated to be in charge of Cyber issues aboard ship, e.g., training, instructions, protection measures?
    - ☐ Department Head
    - ☐ Division Officer
    - ☐ CPO
    - ☐ Other: _____

20. How is this person designated?
    - ☐ Primary Duty
    - ☐ Collateral Duty
    - ☐ Other: _____

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

21. Cyber threats can potentially affect each Department to varying degrees, rank the following Departments according to their overall sensitivity to such a threat (1—least sensitive, 2—less sensitive, 3—sensitive, 4—more sensitive, 5—most sensitive):

| | | | | | |
|---|---|---|---|---|---|
| Administrative | 1 | 2 | 3 | 4 | 5 |
| Combat Systems | 1 | 2 | 3 | 4 | 5 |
| Engineering | 1 | 2 | 3 | 4 | 5 |
| Operations | 1 | 2 | 3 | 4 | 5 |
| Weapons | 1 | 2 | 3 | 4 | 5 |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

22. Which Department should oversee Cyber issues, including protection, policy, training, etc.?
- ☐ Administrative
- ☐ Combat Systems
- ☐ Engineering
- ☐ Operations
- ☐ Weapons
- ☐ Other: _____

23. Should the Department in charge of Cyber have a counterpart on Staff?
- ☐ Yes
- ☐ No

24. Should more Cyber Training be given to unrestricted line (URL) Officers?
- ☐ Yes
- ☐ No

25. If yes, when should Cyber Training be given (check all that apply)?
- ☐ Basic Division Officer Course
- ☐ DH School
- ☐ XO/CO School
- ☐ Other: _____

Additional Comments on Shipboard Network Concerns:

_____

_____

_____

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

***Further Addressing Shipboard Network Concerns***

26. Rate each methods' potential to improve a crew's ability to deal with cyber threats (1—lowest potential, 2—lower potential, 3—average potential, 4—higher potential, 5—highest potential):

| | | | | | |
|---|---|---|---|---|---|
| All Hands Training | 1 | 2 | 3 | 4 | 5 |
| Early Warning Detection Systems, type _____ | 1 | 2 | 3 | 4 | 5 |
| Outsourcing Systems and Maintenance | 1 | 2 | 3 | 4 | 5 |
| Schooling for Operators | 1 | 2 | 3 | 4 | 5 |
| Use of Commercial Off-The-Shelf (COTS) Systems | 1 | 2 | 3 | 4 | 5 |
| Covert Analysis Detection System (CADS) | 1 | 2 | 3 | 4 | 5 |
| Simulators | 1 | 2 | 3 | 4 | 5 |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Further Addressing Shipboard Network Concerns:

_____
_____
_____

***Additional Information***

Additional Comments / Suggestions:

_____
_____
_____
_____

When you are done, please e-mail the survey back to me at szielech@nps.edu.

***Thank you for your participation!***

# APPENDIX C. RESPONDENT A, FFG CO

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

## Tactics for Protecting Shipboard IT Networks

***Purpose***: Data gathered here will be used to build upon previous NPS theses that presented Covert Analysis Detection (CAD) System as a viable option for the defense of ships from cyber attacks.

### *General Information*

1. Rank at time of At-Sea Command (check all that apply):
   - ☐ Lieutenant (LT)
   - ☐ Lieutenant Commander (LCDR)
   - ☐ Commander (CDR)
   - ☐ Captain (CAPT)

2. Type of ship (check all that apply):
   - ☐ Amphibious Ship, type _____
   - ☐ Cruiser (CG)
   - ☐ Destroyer (DDG)
   - ☐ Frigate (FFG)
   - ☐ Littoral Combat Ship (LCS)
   - ☐ Other, type _____

3. Weapons Department / Combat Systems Department experience:
   - ☐ Yes
   - ☐ No

4. Were any ships BMD capable?
   - ☐ Yes
   - ☐ No

5. Number of At-Sea Commands:
   - ☐ None
   - ☐ One
   - ☐ Two
   - ☐ Three
   - ☐ Four or more

### *Ship Specific Concerns*

6. Rank each ship's vulnerability to cyber related attacks (1—least, 5—most):

| | | | | | |
|---|---|---|---|---|---|
| Amphibious Ship, type _____ | 1 | 2 | 3 | 4 | 5 |
| Cruiser (CG) | 1 | 2 | 3 | 4 | 5 |
| Destroyer (DDG) | 1 | 2 | 3 | 4 | 5 |
| Frigate (FFG) | 1 | 2 | 3 | 4 | 5 |
| Littoral Combat Ship (LCS) | 1 | 2 | 3 | 4 | 5 |
| Other, type _____ | 1 | 2 | 3 | 4 | 5 |

7. Which ship type is currently most vulnerable to cyber attack?
   - ☐ Amphibious Ship, type _____
   - ☐ Cruiser (CG)
   - ☐ Destroyer (DDG)
   - ☐ Frigate (FFG)
   - ☐ Littoral Combat Ship (LCS)
   - ☐ Other, type _____
   - ☐ No Difference

8. Which ship type is currently least vulnerable to cyber attack?
   - ☐ Amphibious Ship, type _____
   - ☐ Cruiser (CG)
   - ☐ Destroyer (DDG)
   - ☐ Frigate (FFG)
   - ☐ Littoral Combat Ship (LCS)
   - ☐ Other, type _____
   - ☐ No Difference

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

Additional Comments on Ship Specific Concerns:

I think all ships with networks and continuous IP bandwidth are equally vulnerable. However, I think that the more networks and certainly Aegis ships with networks that connect to the combat system, the more catastrophic the impact of a network intrusion.

***Cyber Threats***

9. While in Command, did you view cyber terrorism as a threat?
   - ☐ Yes
   - ☐ No

10. Do you view cyber terrorism as a threat?
    - ☐ Currently (within next 10 years)
    - ☐ In the future (over 10 years away)

11. When is a ship most vulnerable?
    - ☐ Homeport
    - ☐ Port Visits
    - ☐ Deployment
    - ☐ Exercises
    - ☐ Other: _No Difference___

12. When is a ship least vulnerable?
    - ☐ Homeport
    - ☐ Port Visits
    - ☐ Deployment
    - ☐ Exercises

    Other: _No Difference_____

13. Should ships refrain from Wi-Fi use while in port to avoid potential cyber attacks?
    - ☐ Yes
    - ☐ No

Additional Comments on Cyber Threats:

I think that anytime a ship has IP bandwidth, they are vulnerable to attack. However, being on deployment or involved in a major, publicized exercise would certainly increase the likelihood that a specific ship or unit would be targeted for attack. For instance, FDNF ships are more likely to be attacked by certain actors than ships homeported in Mayport.

***Cyber Protection Implementation & Necessity***

14. Given the potential for cyber attack, rank each method of implementing a cyber protection program/system (e.g., Covert Analysis Detection (CAD) System[1]), would be effective (1—least, 5—most):

| | | | | | |
|---|---|---|---|---|---|
| By Ship Type | 1 | 2 | 3 | 4 | 5 |
| By Numbered Fleet | 1 | 2 | 3 | 4 | 5 |
| Pre Deployment Pacakge | 1 | 2 | 3 | 4 | 5 |
| During Mid-life Upgrade | 1 | 2 | 3 | 4 | 5 |
| During Intial Building | 1 | 2 | 3 | 4 | 5 |

[1] "A CAD (Covert Analysis Detection) system is a sensor or sensor system that can covertly capture incoming and outgoing data while analyzing and maintaining control of the data." —Adderson, O. G. and K. A. Wood. (2010). *A Qualitative Analysis of Strategic Capabilities for a Covert Analysis Detection System Onboard an AEGIS Class Ship*. Monterey, Calif.: Naval Postgraduate School.

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

| | | | | | |
|---|---|---|---|---|---|
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Cyber Protection Implementation & Necessity:

I think installing such a system during construction or mid-life upgrade gives the greatest probability of successful integration with ship systems and networks. Performing the install as an AIT (by ship/fleet) is likely to result in a less-effective, add-on vice an integrated system.

### *Fiscal Concerns*

15. Given fiscal constraints, it is necessary to prioritize process/system implementation, upgrade, and training. Prioritize the below areas in regards to Cyber protection of ships (1—lowest priority, 5—highest priority):

| | | | | | |
|---|---|---|---|---|---|
| Offensive, e.g., Protecting against Cyber Attacks | 1 | 2 | 3 | 4 | 5 |
| Training, e.g., Cyber | 1 | 2 | 3 | 4 | 5 |
| Maintenance, e.g., Cyber Protection Infrastructure | 1 | 2 | 3 | 4 | 5 |
| Defensive, e.g., Install Cyber Protection Systems/Processes | 1 | 2 | 3 | 4 | 5 |
| Guidance, e.g., Cyber Implementation/Protection Policy | 1 | 2 | 3 | 4 | 5 |
| Other Areas of Cyber Concern: _____ | 1 | 2 | 3 | 4 | 5 |

16. Rank the below methods of implementation to increase cyber protection through systems/processes:

| | | | | | |
|---|---|---|---|---|---|
| Fleetwide | 1 | 2 | 3 | 4 | 5 |
| Deployed Platforms Only | 1 | 2 | 3 | 4 | 5 |
| Only When a Threat is Deemed Imminent | 1 | 2 | 3 | 4 | 5 |
| Platform Specific (which: _____) | 1 | 2 | 3 | 4 | 5 |
| Other Method: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Fiscal Concerns:

### *Shipboard Network Concerns*

17. Which system is most vulnerable to cyber attack or cyber intrusion?
- ☐ Combat Systems
- ☐ Communications
- ☐ Engineering
- ☐ Navigation
- ☐ Weapons
- ☐ Other: _____

18. Which system is least vulnerable to cyber attack or cyber intrusion?
- ☐ Combat Systems
- ☐ Communications
- ☐ Engineering
- ☐ Navigation
- ☐ Weapons
- ☐ Other: _____

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

19. Who is usually designated to be in charge of Cyber Threat?
- ☐ Department Head
- ☐ Division Officer
- ☐ CPO
- ☐ Other: _____

20. How is this person designated?
- ☐ Primary Duty
- ☐ Collateral Duty
- ☐ Other: _____

21. Cyber threats can potentially affect each Department to varying degrees, rank each Department's sensitivity to such a threat (1—least, 5—most):

| | | | | | |
|---|---|---|---|---|---|
| Combat Systems | 1 | 2 | 3 | 4 | 5 |
| Operations | 1 | 2 | 3 | 4 | 5 |
| Engineering | 1 | 2 | 3 | 4 | 5 |
| Administrative | 1 | 2 | 3 | 4 | 5 |
| Weapons | 1 | 2 | 3 | 4 | 5 |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

22. Which Department should oversee Cyber protection and policy?
- ☐ Combat Systems
- ☐ Operations
- ☐ Engineering
- ☐ Administrative
- ☐ Weapons
- ☐ Other: _____

23. Should the Department in charge of Cyber have a counterpart on Staff?
- ☐ Yes
- ☐ No

24. Should increased Cyber Training be given to unrestricted line (URL) Officers?
- ☐ Yes
- ☐ No

25. If yes, when should Cyber Training be given (check all that apply)?
- ☐ SWOS
- ☐ DH School
- ☐ XO/CO School
- ☐ Other: _____

Additional Comments on Shipboard Network Concerns:

I strongly believe that cyber training for the URL community, specifically SWO, is lacking. We need to teach it like 3M; Basic training for Divos, advanced training for DHs, and executive training for CO/XO.

***Further Addressing Shipboard Network Concerns***

1. Rank each methods potential to help better prepare shipboard personnel for dealing with potential cyber threats (1—lowest, 5—highest):

| | | | | | |
|---|---|---|---|---|---|
| All Hands Training | 1 | 2 | 3 | 4 | 5 |
| Early Warning Detection Systems, type _____ | 1 | 2 | 3 | 4 | 5 |
| Outsourcing Systems and Maintenance | 1 | 2 | 3 | 4 | 5 |

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

| | | | | | |
|---|---|---|---|---|---|
| Schooling for Operators | 1 | 2 | 3 | 4 | 5 |
| Use of COTS | 1 | 2 | 3 | 4 | 5 |
| Covert Analysis Detection System (CADS) | 1 | 2 | 3 | 4 | 5 |
| Simulators | 1 | 2 | 3 | 4 | 5 |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Further Addressing Shipboard Network Concerns:

_____

_____

_____

***Additional Information***

Additional Comments / Suggestions:

_____

_____

_____

_____

When you are done, please e-mail the survey back to me at szielech@nps.edu.

***Thank you for your participation!***

THIS PAGE INTENTIONALLY LEFT BLANK

# APPENDIX D. RESPONDENT B, FFG CO

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

## Tactics for Protecting Shipboard IT Networks

***Purpose***: Data gathered here will be used to build upon previous NPS theses that presented Covert Analysis Detection (CAD) System as a viable option for the defense of ships from cyber attacks.

***General Information***

1. Rank at time of At-Sea Command (check all that apply):
   - ☐ Lieutenant (LT)
   - ☐ Lieutenant Commander (LCDR)
   - X Commander (CDR)
   - ☐ Captain (CAPT)

2. Type of ship (check all that apply):
   - ☐ Amphibious Ship, type _____
   - ☐ Cruiser (CG)
   - ☐ Destroyer (DDG)
   - X Frigate (FFG)
   - ☐ Littoral Combat Ship (LCS)
   - ☐ Other, type _____

3. Weapons Department / Combat Systems Department experience:
   - ☐ Yes
   - XNo

4. Were any ships BMD capable?
   - ☐ Yes
   - ☐ No

5. Number of At-Sea Commands:
   - ☐ None
   - XOne
   - ☐ Two
   - ☐ Three
   - ☐ Four or more

***Ship Specific Concerns***

6. Rank each ship's vulnerability to cyber related attacks (1—least, 5—most):

| | | | | | |
|---|---|---|---|---|---|
| Amphibious Ship, type _____ | 1 | 2 | 3 | **4** | 5 |
| Cruiser (CG) | 1 | 2 | 3 | **4** | 5 |
| Destroyer (DDG) | 1 | 2 | 3 | **4** | 5 |
| Frigate (FFG) | 1 | 2 | 3 | 4 | **5** |
| Littoral Combat Ship (LCS) | 1 | 2 | 3 | **4** | 5 |
| Other, type _____ | 1 | 2 | 3 | 4 | 5 |

7. Which ship type is currently most vulnerable to cyber attack?
   - ☐ Amphibious Ship, type _____
   - ☐ Cruiser (CG)
   - ☐ Destroyer (DDG)
   - X Frigate (FFG)
   - ☐ Littoral Combat Ship (LCS)
   - ☐ Other, type _____
   - ☐ No Difference

8. Which ship type is currently least vulnerable to cyber attack?
   - ☐ Amphibious Ship, type _____
   - ☐ Cruiser (CG)
   - ☐ Destroyer (DDG)
   - ☐ Frigate (FFG)
   - ☐ Littoral Combat Ship (LCS)
   - ☐ Other, type _____
   - X No Difference

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

Additional Comments on Ship Specific Concerns:
FFGs have been equipped with ad hoc systems and have limited connectivity to download patches.

***Cyber Threats***

9. While in Command, did you view cyber terrorism as a threat?
   - ☐ Yes
   - X No

10. Do you view cyber terrorism as a threat?
    - X Currently (within next 10 years)
    - ☐ In the future (over 10 years away)

11. When is a ship most vulnerable?
    - X Homeport
    - ☐ Port Visits
    - ☐ Deployment
    - ☐ Exercises
    - ☐ Other: _____

12. When is a ship least vulnerable?
    - ☐ Homeport
    - ☐ Port Visits
    - ☐ Deployment
    - X Exercises
    - Other: _____

13. Should ships refrain from Wi-Fi use while in port to avoid potential cyber attacks?
    - X Yes
    - ☐ No

Additional Comments on Cyber Threats:
Ships are least vulnerable in exercises, because they are expecting to be probed by red cells.

***Cyber Protection Implementation & Necessity***

14. Given the potential for cyber attack, rank each method of implementing a cyber protection program/system (e.g., Covert Analysis Detection (CAD) System[1]), would be effective (1—least, 5—most):

| | | | | | |
|---|---|---|---|---|---|
| By Ship Type | 1 | 2 | **3** | 4 | 5 |
| By Numbered Fleet | 1 | **2** | 3 | 4 | **5** |
| Pre Deployment Package | **1** | 2 | 3 | 4 | 5 |
| During Mid-life Upgrade | 1 | 2 | 3 | **4** | 5 |
| During Initial Building | 1 | 2 | 3 | 4 | **5** |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Cyber Protection Implementation & Necessity:

[1] "A CAD (Covert Analysis Detection) system is a sensor or sensor system that can covertly capture incoming and outgoing data while analyzing and maintaining control of the data." —Adderson, O. G. and K. A. Wood. (2010). *A Qualitative Analysis of Strategic Capabilities for a Covert Analysis Detection System Onboard an AEGIS Class Ship*. Monterey, Calif.: Naval Postgraduate School.

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

### *Fiscal Concerns*

15. Given fiscal constraints, it is necessary to prioritize process/system implementation, upgrade, and training. Prioritize the below areas in regards to Cyber protection of ships (1—lowest priority, 5—highest priority):

| | | | | | |
|---|---|---|---|---|---|
| Offensive, e.g., Protecting against Cyber Attacks | 1 | 2 | 3 | **4** | 5 |
| Training, e.g., Cyber | 1 | 2 | 3 | **4** | 5 |
| Maintenance, e.g., Cyber Protection Infrastructure | 1 | 2 | 3 | 4 | **5** |
| Defensive, e.g., Install Cyber Protection Systems/Processes | 1 | 2 | 3 | 4 | **5** |
| Guidance, e.g., Cyber Implementation/Protection Policy | 1 | **2** | 3 | 4 | 5 |
| Other Areas of Cyber Concern: _____ | **1** | 2 | 3 | 4 | 5 |

16. Rank the below methods of implementation to increase cyber protection through systems/processes:

| | | | | | |
|---|---|---|---|---|---|
| Fleetwide | 1 | 2 | 3 | 4 | **5** |
| Deployed Platforms Only | 1 | 2 | **3** | 4 | 5 |
| Only When a Threat is Deemed Imminent | **1** | 2 | 3 | 4 | 5 |
| Platform Specific (which: _____) | 1 | 2 | 3 | **4** | 5 |
| Other Method: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Fiscal Concerns:
If you implement only when a threat is imminent, it is too late.

### *Shipboard Network Concerns*

17. Which system is most vulnerable to cyber attack or cyber intrusion?
- ☐ Combat Systems
- X Communications
- ☐ Engineering
- ☐ Navigation
- ☐ Weapons
- ☐ Other: _____

18. Which system is least vulnerable to cyber attack or cyber intrusion?
- ☐ Combat Systems
- ☐ Communications
- X Engineering
- ☐ Navigation
- ☐ Weapons
- ☐ Other: _____

19. Who is usually designated to be in charge of Cyber Threat?
- ☐ Department Head
- ☐ Division Officer
- ☐ CPO
- X Other: IT1 with the network NEC_____

20. How is this person designated?
- ☐ Primary Duty
- X Collateral Duty
- ☐ Other: _____

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

21. Cyber threats can potentially affect each Department to varying degrees, rank each Department's sensitivity to such a threat (1—least, 5—most):

| | | | | | |
|---|---|---|---|---|---|
| Combat Systems | 1 | 2 | **3** | 4 | 5 |
| Operations | 1 | 2 | 3 | 4 | **5** |
| Engineering | **1** | 2 | 3 | 4 | 5 |
| Administrative | 1 | 2 | 3 | **4** | 5 |
| Weapons | 1 | **2** | 3 | 4 | 5 |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

22. Which Department should oversee Cyber protection and policy?
- ☐ Combat Systems
- X Operations
- ☐ Engineering
- ☐ Administrative
- ☐ Weapons
- ☐ Other: _____

23. Should the Department in charge of Cyber have a counterpart on Staff?
- X Yes
- ☐ No

24. Should increased Cyber Training be given to unrestricted line (URL) Officers?
- X Yes
- ☐ No

25. If yes, when should Cyber Training be given (check all that apply)?
- X SWOS
- X DH School
- X XO/CO School
- ☐ Other: _____

Additional Comments on Shipboard Network Concerns:
There has not generally been a lot of oversight on cyber defense; however, RADM Thomas (CNSL) has recently been emphasizing the need to have CO-level oversight on this issue.

***Further Addressing Shipboard Network Concerns***

1. Rank each methods potential to help better prepare shipboard personnel for dealing with potential cyber threats (1—lowest, 5—highest):

| | | | | | |
|---|---|---|---|---|---|
| All Hands Training | 1 | 2 | **3** | 4 | 5 |
| Early Warning Detection Systems, type _____ | 1 | 2 | 3 | 4 | **5** |
| Outsourcing Systems and Maintenance | 1 | **2** | 3 | 4 | 5 |
| Schooling for Operators | 1 | 2 | **3** | 4 | 5 |
| Use of COTS | 1 | 2 | **3** | 4 | 5 |
| Covert Analysis Detection System (CADS) | 1 | 2 | 3 | 4 | **5** |
| Simulators | 1 | 2 | 3 | **4** | 5 |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

Additional Comments on Further Addressing Shipboard Network Concerns:

_____

_____

_____

***Additional Information***

Additional Comments / Suggestions:

_____

_____

_____

_____

When you are done, please e-mail the survey back to me at szielech@nps.edu.

***Thank you for your participation!***

THIS PAGE INTENTIONALLY LEFT BLANK

# APPENDIX E. RESPONDENT C, FFG CO

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

## Tactics for Protecting Shipboard IT Networks

***Purpose***: Data gathered here will be used to build upon previous NPS theses that presented Covert Analysis Detection (CAD) System as a viable option for the defense of ships from cyber attacks.

***General Information***

1. Rank at time of At-Sea Command (check all that apply):
   X Lieutenant (LT)
   X Lieutenant Commander (LCDR)
   X Commander (CDR)
   ☐ Captain (CAPT)

2. Type of ship (check all that apply):
   ☐ Amphibious Ship, type _____
   ☐ Cruiser (CG)
   ☐ Destroyer (DDG)
   X Frigate (FFG)
   ☐ Littoral Combat Ship (LCS)
   ☐ Other, type PC/MCM_____

3. Weapons Department / Combat Systems Department experience:
   X Yes
   ☐ No

4. Were any ships BMD capable?
   ☐ Yes
   X No

5. Number of At-Sea Commands:
   ☐ None
   ☐ One
   ☐ Two
   X Three
   ☐ Four or more

***Ship Specific Concerns***

6. Rank each ship's vulnerability to cyber related attacks (1—least, 5—most):

| | | | | | |
|---|---|---|---|---|---|
| Amphibious Ship, type _____ | 1 | X | 3 | 4 | 5 |
| Cruiser (CG) | 1 | 2 | 3 | x | 5 |
| Destroyer (DDG) | 1 | 2 | X | 4 | 5 |
| Frigate (FFG) | x | 2 | 3 | 4 | 5 |
| Littoral Combat Ship (LCS) | 1 | 2 | 3 | 4 | X |
| Other, type _____ | 1 | 2 | 3 | 4 | X |

7. Which ship type is currently most vulnerable to cyber attack?
   ☐ Amphibious Ship, type _____
   ☐ Cruiser (CG)
   ☐ Destroyer (DDG)
   ☐ Frigate (FFG)
   xLittoral Combat Ship (LCS)
   ☐ Other, type _____
   No Difference

8. Which ship type is currently least vulnerable to cyber attack?
   ☐ Amphibious Ship, type _____
   ☐ Cruiser (CG)
   ☐ Destroyer (DDG)
   xFrigate (FFG)
   ☐ Littoral Combat Ship (LCS)
   ☐ Other, type _____
   No Difference

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

Additional Comments on Ship Specific Concerns:
Any ship's network that connects to an outside network (such as NIPRNET) is vulnerable to outside intrusion, denial of service, manipulation, or other malicious interaction.

***Cyber Threats***

9. While in Command, did you view cyber terrorism as a threat?
   - X Yes
   - ☐ No

10. Do you view cyber terrorism as a threat?
    - X Currently (within next 10 years)
    - ☐ In the future (over 10 years away)

11. When is a ship most vulnerable?
    - ☐ Homeport
    - ☐ Port Visits
    - ☐ Deployment
    - ☐ Exercises
    - X Other: when connected

12. When is a ship least vulnerable?
    - ☐ Homeport
    - ☐ Port Visits
    - ☐ Deployment
    - ☐ Exercises
    - Other: _____

13. Should ships refrain from Wi-Fi use while in port to avoid potential cyber attacks?
    - X Yes
    - ☐ No

Additional Comments on Cyber Threats:
WIFI gives an attacker a short-cut to identifying a way into the network when compared to wired/fiber or satellite connectivity.

***Cyber Protection Implementation & Necessity***

14. Given the potential for cyber attack, rank each method of implementing a cyber protection program/system (e.g., Covert Analysis Detection (CAD) System[1]), would be effective (1—least, 5—most):

| | | | | | |
|---|---|---|---|---|---|
| By Ship Type | 1 | 2 | X | 4 | 5 |
| By Numbered Fleet | 1 | 2 | X | 4 | 5 |
| Pre Deployment Pacakge | 1 | 2 | 3 | X | 5 |
| During Mid-life Upgrade | 1 | 2 | X | 4 | 5 |
| During Intial Building | 1 | 2 | 3 | 4 | X |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Cyber Protection Implementation & Necessity:

[1] "A CAD (Covert Analysis Detection) system is a sensor or sensor system that can covertly capture incoming and outgoing data while analyzing and maintaining control of the data." —Adderson, O. G. and K. A. Wood. (2010). *A Qualitative Analysis of Strategic Capabilities for a Covert Analysis Detection System Onboard an AEGIS Class Ship*. Monterey, Calif.: Naval Postgraduate School.

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

***Fiscal Concerns***

15. Given fiscal constraints, it is necessary to prioritize process/system implementation, upgrade, and training. Prioritize the below areas in regards to Cyber protection of ships (1—lowest priority, 5—highest priority):

| | | | | | |
|---|---|---|---|---|---|
| Offensive, e.g., Protecting against Cyber Attacks | 1 | X | 3 | 4 | 5 |
| Training, e.g., Cyber | 1 | 2 | 3 | 4 | 5 |
| Maintenance, e.g., Cyber Protection Infrastructure | 1 | 2 | 3 | X | 5 |
| Defensive, e.g., Install Cyber Protection Systems/Processes | 1 | 2 | 3 | 4 | X |
| Guidance, e.g., Cyber Implementation/Protection Policy | X | 2 | x | 4 | 5 |
| Other Areas of Cyber Concern: _____ | 1 | 2 | 3 | 4 | 5 |

16. Rank the below methods of implementation to increase cyber protection through systems/processes:

| | | | | | |
|---|---|---|---|---|---|
| Fleetwide | 1 | 2 | 3 | 4 | X |
| Deployed Platforms Only | 1 | 2 | 3 | X | 5 |
| Only When a Threat is Deemed Imminent | X | 2 | 3 | 4 | 5 |
| Platform Specific (which: _____) | 1 | 2 | 3 | 4 | 5 |
| Other Method: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Fiscal Concerns:

***Shipboard Network Concerns***

17. Which system is most vulnerable to cyber attack or cyber intrusion?
- ☐ Combat Systems
- ☐ Communications
- Engineering
- X Navigation
- ☐ Weapons
- ☐ Other: _____

18. Which system is least vulnerable to cyber attack or cyber intrusion?
- ☐ Combat Systems
- ☐ Communications
- ☐ Engineering
- ☐ Navigation
- X Weapons
- ☐ Other: _____

19. Who is usually designated to be in charge of Cyber Threat?
- ☐ Department Head
- ☐ Division Officer
- xCPO
- ☐ Other: _____

20. How is this person designated?
- ☐ Primary Duty
- xCollateral Duty
- ☐ Other: _____

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

21. Cyber threats can potentially affect each Department to varying degrees, rank each Department's sensitivity to such a threat (1—least, 5—most):

| | | | | | |
|---|---|---|---|---|---|
| Combat Systems | 1 | 2 | 3 | X | 5 |
| Operations | 1 | 2 | 3 | 4 | X |
| Engineering | 1 | 2 | 3 | 4 | X |
| Administrative | 1 | 2 | 3 | 4 | X |
| Weapons | 1 | 2 | 3 | X | 5 |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

22. Which Department should oversee Cyber protection and policy?
- ☐ Combat Systems
- xOperations
- ☐ Engineering
- ☐ Administrative
- ☐ Weapons
- ☐ Other: _____

23. Should the Department in charge of Cyber have a counterpart on Staff?
- xYes
- ☐ No

24. Should increased Cyber Training be given to unrestricted line (URL) Officers?
- xYes
- ☐ No

25. If yes, when should Cyber Training be given (check all that apply)?
- xSWOS
- xDH School
- xXO/CO School
- xOther: _every opportunity_____

Additional Comments on Shipboard Network Concerns:

_____

_____

_____

***Further Addressing Shipboard Network Concerns***

1. Rank each methods potential to help better prepare shipboard personnel for dealing with potential cyber threats (1—lowest, 5—highest):

| | | | | | |
|---|---|---|---|---|---|
| All Hands Training | 1 | 2 | 3 | 4 | X |
| Early Warning Detection Systems, type _____ | 1 | 2 | 3 | 4 | 5 |
| Outsourcing Systems and Maintenance | x | 2 | 3 | 4 | 5 |
| Schooling for Operators | 1 | 2 | 3 | X | 5 |
| Use of COTS | 1 | 2 | 3 | 4 | 5 |
| Covert Analysis Detection System (CADS) | 1 | 2 | 3 | 4 | 5 |
| Simulators | 1 | 2 | 3 | 4 | 5 |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

Additional Comments on Further Addressing Shipboard Network Concerns:

_____

_____

_____

***Additional Information***

Additional Comments / Suggestions:

Rephrase your questions. Define your terms to reduce my speculation.

_____

_____

_____

When you are done, please e-mail the survey back to me at szielech@nps.edu.

***Thank you for your participation!***

THIS PAGE INTENTIONALLY LEFT BLANK

# APPENDIX F. RESPONDENT D, CG CO

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

## Tactics for Protecting Shipboard IT Networks

***Purpose***: Data gathered here will be used to build upon previous NPS theses that presented Covert Analysis Detection (CAD) System as a viable option for the defense of ships from cyber attacks.

***General Information***

1. Rank at time of At-Sea Command (check all that apply):
   xLieutenant (LT)
   xLieutenant Commander (LCDR)
   xCommander (CDR)
   xCaptain (CAPT)

2. Type of ship (check all that apply):
   ☐ Amphibious Ship, type _____
   xCruiser (CG)
   xDestroyer (DDG)
   xFrigate (FFG)
   ☐ Littoral Combat Ship (LCS)
   xOther, type __PC_____

3. Weapons Department / Combat Systems Department experience:
   xYes
   ☐ No

4. Were any ships BMD capable?
   ☐ Yes
   xNo

5. Number of At-Sea Commands:
   ☐ None
   ☐ One
   ☐ Two
   ☐ Three
   xFour or more

***Ship Specific Concerns***

6. Rank each ship's vulnerability to cyber related attacks (1—least, 5—most):

| | | | | | |
|---|---|---|---|---|---|
| Amphibious Ship, type _____ | 1 | 2 | 3 | 4 | x |
| Cruiser (CG) | 1 | 2 | 3 | 4 | x |
| Destroyer (DDG) | 1 | 2 | 3 | 4 | 5 |
| Frigate (FFG) | 1 | 2 | 3 | 4 | x |
| Littoral Combat Ship (LCS) | 1 | 2 | 3 | 4 | 5 |
| Other, type _____Patrol Coastal | 1 | 2 | 3 | 4 | x |

7. Which ship type is currently most vulnerable to cyber attack?
   ☐ Amphibious Ship, type _____
   ☐ Cruiser (CG)
   ☐ Destroyer (DDG)
   ☐ Frigate (FFG)
   ☐ Littoral Combat Ship (LCS)
   ☐ Other, type _____
   xNo Difference

8. Which ship type is currently least vulnerable to cyber attack?
   ☐ Amphibious Ship, type _____
   ☐ Cruiser (CG)
   ☐ Destroyer (DDG)
   ☐ Frigate (FFG)
   ☐ Littoral Combat Ship (LCS)
   ☐ Other, type _____
   xNo Difference

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

Additional Comments on Ship Specific Concerns:

Social Engineering Threats, Zeus Type Threats, Stuxnet Type Threats, Hacking the homefront, Hacking the MSC Logistics Fleet (no gas is a mission kill), civilian infrastructures lack of focus, China and Russia's (now Irans) eagerness to disrupt our systems is not resulting in effective systems to defeat the threats. AIS for example is relied upon as a "IFF" tool which it is not. IP professionals worried too much about warfare pins and not enough about bots, Trojans, and Advanced Persistent Threats (APTs)

***Cyber Threats***

9. While in Command, did you view cyber terrorism as a threat?
   xYes
   ☐ No
10. Do you view cyber terrorism as a threat?
    xCurrently (within next 10 years)
    ☐ In the future (over 10 years away)
11. When is a ship most vulnerable?
    ☐ Homeport
    ☐ Port Visits
    ☐ Deployment
    ☐ Exercises
    xOther: _Doesn't matter when!_____
12. When is a ship least vulnerable?
    ☐ Homeport
    ☐ Port Visits
    ☐ Deployment
    ☐ Exercises
    Other: __See 11_____
13. Should ships refrain from Wi-Fi use while in port to avoid potential cyber attacks?
    ☐ Yes
    xNo Figure a way to use it safely!

Additional Comments on Cyber Threats:

I have AQD's for Information Operations Commander and Planner earned during STO tours at USSOCOM. This threat is real, ships are extremely vulnerable, and more importantly we have yet to fully integrate Cyber effects within JADOCS to engage within OPLAN Development (I have a White Paper ☺

***Cyber Protection Implementation & Necessity***

14. Given the potential for cyber attack, rank each method of implementing a cyber protection program/system (e.g., Covert Analysis Detection (CAD) System[1]), would be effective (1—least, 5—most):

| | | | | | |
|---|---|---|---|---|---|
| By Ship Type | 1 | 2 | 3 | 4 | x |
| By Numbered Fleet | 1 | 2 | 3 | 4 | x |
| Pre Deployment Pacakge | 1 | 2 | 3 | 4 | x |
| During Mid-life Upgrade | 1 | 2 | x | 4 | 5 |

[1] "A CAD (Covert Analysis Detection) system is a sensor or sensor system that can covertly capture incoming and outgoing data while analyzing and maintaining control of the data." —Adderson, O. G. and K. A. Wood. (2010). *A Qualitative Analysis of Strategic Capabilities for a Covert Analysis Detection System Onboard an AEGIS Class Ship*. Monterey, Calif.: Naval Postgraduate School.

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

| | | | | | |
|---|---|---|---|---|---|
| During Intial Building | 1 | 2 | 3 | 4 | x |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Cyber Protection Implementation & Necessity:

The CAD needs to include advanced data visualization strategies, neural network algorithms' that adapt and detect zero day threats, and more.

***Fiscal Concerns***

15. Given fiscal constraints, it is necessary to prioritize process/system implementation, upgrade, and training. Prioritize the below areas in regards to Cyber protection of ships (1—lowest priority, 5—highest priority):

| | | | | | |
|---|---|---|---|---|---|
| Offensive, e.g., Protecting against Cyber Attacks | 1 | 2 | x | 4 | 5 |
| Training, e.g., Cyber | 1 | 2 | 3 | 4 | x |
| Maintenance, e.g., Cyber Protection Infrastructure | 1 | 2 | x | 4 | 5 |
| Defensive, e.g., Install Cyber Protection Systems/Processes | 1 | 2 | x | 4 | 5 |
| Guidance, e.g., Cyber Implementation/Protection Policy | 1 | 2 | 3 | 4 | x |
| Other Areas of Cyber Concern: _____Homefront Hacking | 1 | 2 | 3 | 4 | x |

16. Rank the below methods of implementation to increase cyber protection through systems/processes:

| | | | | | |
|---|---|---|---|---|---|
| Fleetwide | 1 | 2 | 3 | 4 | x |
| Deployed Platforms Only | 1 | 2 | x | 4 | 5 |
| Only When a Threat is Deemed Imminent | x | 2 | 3 | 4 | 5 |
| Platform Specific (which: _____) | 1 | 2 | 3 | 4 | 5 |
| Other Method: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Fiscal Concerns:

This is NOT a concern. Read "Switch". Big problems DO NOT HAVE TO have big solutions. Little best practice concepts are the key to implementing big change.

***Shipboard Network Concerns***

17. Which system is most vulnerable to cyber attack or cyber intrusion?
- ☐ Combat Systems
- xCommunications
- xEngineering
- xNavigation
- ☐ Weapons
- ☐ Other: _____

18. Which system is least vulnerable to cyber attack or cyber intrusion?
- xCombat Systems
- ☐ Communications
- ☐ Engineering
- ☐ Navigation
- xWeapons
- ☐ Other: _____

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

19. Who is usually designated to be in charge of Cyber Threat?
- ☐ Department Head
- ☐ Division Officer
- ☐ CPO
- xOther: On my ships it was me with a hand selected officer._____

20. How is this person designated?
- xPrimary Duty
- ☐ Collateral Duty
- ☐ Other: _____

21. Cyber threats can potentially affect each Department to varying degrees, rank each Department's sensitivity to such a threat (1—least, 5—most):

| | | | | | |
|---|---|---|---|---|---|
| Combat Systems | x | 2 | 3 | 4 | 5 |
| Operations | 1 | 2 | 3 | 4 | x |
| Engineering | 1 | 2 | 3 | x | 5 |
| Administrative | 1 | 2 | 3 | 4 | x |
| Weapons | 1 | 2 | x | 4 | 5 |
| Other: _____Supply! They will KILL US HERE! | 1 | 2 | 3 | 4 | x |

22. Which Department should oversee Cyber protection and policy?
- X Combat Systems
- xOperations
- ☐ Engineering
- ☐ Administrative
- ☐ Weapons
- ☐ Other: _____

23. Should the Department in charge of Cyber have a counterpart on Staff?
- X Yes
- ☐ No

24. Should increased Cyber Training be given to unrestricted line (URL) Officers?
- xYes
- ☐ No

25. If yes, when should Cyber Training be given (check all that apply)?
- xSWOS
- xDH School
- xXO/CO School
- xOther: _all officers___

Additional Comments on Shipboard Network Concerns:

We must look holistically at the threat and the systems. I can degrade mission success in multiple ways, we seldom look at vectors of attack in a holistic way.

***Further Addressing Shipboard Network Concerns***

1. Rank each methods potential to help better prepare shipboard personnel for dealing with potential cyber threats (1—lowest, 5—highest):

| | | | | | |
|---|---|---|---|---|---|
| All Hands Training | 1 | 2 | 3 | 4 | x |
| Early Warning Detection Systems, type _____ | 1 | 2 | 3 | x | 5 |
| Outsourcing Systems and Maintenance | 1 | 2 | x | 4 | 5 |

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

| | | | | | |
|---|---|---|---|---|---|
| Schooling for Operators | 1 | 2 | 3 | 4 | x |
| Use of COTS | 1 | 2 | 3 | x | 5 |
| Covert Analysis Detection System (CADS) | 1 | 2 | 3 | x | 5 |
| Simulators – I would like to build an Agent-based PKI training tool to make this happen. | 1 | 2 | 3 | 4 | x |
| Other: _____Data visualization. I get better data about the weather and virus at CDC than I do about the cyber threat. | 1 | 2 | 3 | 4 | x |

Additional Comments on Further Addressing Shipboard Network Concerns:

_____

_____

_____

***Additional Information***

Additional Comments / Suggestions:

Let's talk.

_____

_____

_____

_____

When you are done, please e-mail the survey back to me at szielech@nps.edu.

***Thank you for your participation!***

THIS PAGE INTENTIONALLY LEFT BLANK

# APPENDIX G. RESPONDENT E, FFG CO

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

## Tactics for Protecting Shipboard IT Networks

***Purpose***: Data gathered here will be used to build upon previous NPS theses that presented Covert Analysis Detection (CAD) System as a viable option for the defense of ships from cyber attacks.

### *General Information*

1. Rank at time of At-Sea Command (check all that apply):
   - ☐ Lieutenant (LT)
   - ☐ Lieutenant Commander (LCDR)
   - ☑ Commander (CDR)
   - ☐ Captain (CAPT)

2. Type of ship (check all that apply):
   - ☐ Amphibious Ship, type _____
   - ☐ Cruiser (CG)
   - ☐ Destroyer (DDG)
   - ☑ Frigate (FFG)
   - ☐ Littoral Combat Ship (LCS)
   - ☐ Other, type _____

3. Weapons Department / Combat Systems Department experience:
   - ☐ Yes
   - ☑ No

4. Were any ships BMD capable?
   - ☐ Yes
   - ☑ No

5. Number of At-Sea Commands:
   - ☐ None
   - ☑ One
   - ☐ Two
   - ☐ Three
   - ☐ Four or more

### *Ship Specific Concerns*

6. Rank each ship's vulnerability to cyber related attacks (1—least, 5—most):

| | | | | | |
|---|---|---|---|---|---|
| Amphibious Ship, type ALL | 1 | 2 | (3) | 4 | 5 |
| Cruiser (CG) | 1 | 2 | (3) | 4 | 5 |
| Destroyer (DDG) | 1 | 2 | (3) | 4 | 5 |
| Frigate (FFG) | 1 | 2 | (3) | 4 | 5 |
| Littoral Combat Ship (LCS) | 1 | 2 | (3) | 4 | 5 |
| Other, type _____ | 1 | 2 | (3) | 4 | 5 |

7. Which ship type is currently most vulnerable to cyber attack?
   - ☐ Amphibious Ship, type _____
   - ☐ Cruiser (CG)
   - ☐ Destroyer (DDG)
   - ☐ Frigate (FFG)
   - ☐ Littoral Combat Ship (LCS)
   - ☐ Other, type _____
   - ☑ No Difference

8. Which ship type is currently least vulnerable to cyber attack?
   - ☐ Amphibious Ship, type _____
   - ☐ Cruiser (CG)
   - ☐ Destroyer (DDG)
   - ☐ Frigate (FFG)
   - ☐ Littoral Combat Ship (LCS)
   - ☐ Other, type _____
   - ☑ No Difference

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

Additional Comments on Ship Specific Concerns:

### *Cyber Threats*

9. While in Command, did you view cyber terrorism as a threat?
   - ☑ Yes
   - ☐ No
10. Do you view cyber terrorism as a threat?
    - ☑ Currently (within next 10 years)
    - ☐ In the future (over 10 years away)
11. When is a ship most vulnerable?
    - ☐ Homeport
    - ☑ Port Visits
    - ☐ Deployment
    - ☐ Exercises
    - ☐ Other: _____
12. When is a ship least vulnerable?
    - ☑ Homeport
    - ☐ Port Visits
    - ☐ Deployment
    - ☐ Exercises

    Other: _____
13. Should ships refrain from Wi-Fi use while in port to avoid potential cyber attacks?
    - ☑ Yes
    - ☐ No

Additional Comments on Cyber Threats:

### *Cyber Protection Implementation & Necessity*

14. Given the potential for cyber attack, rank each method of implementing a cyber protection program/system (e.g., Covert Analysis Detection (CAD) System[1]), would be effective (1—least, 5—most):

| | | | | | |
|---|---|---|---|---|---|
| By Ship Type | (1) | 2 | 3 | 4 | 5 |
| By Numbered Fleet | 1 | (2) | 3 | 4 | 5 |
| Pre Deployment Pacakge | 1 | 2 | (3) | 4 | 5 |
| During Mid-life Upgrade | 1 | 2 | 3 | (4) | 5 |
| During Intial Building | 1 | 2 | 3 | 4 | (5) |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Cyber Protection Implementation & Necessity:

[1] "A CAD (Covert Analysis Detection) system is a sensor or sensor system that can covertly capture incoming and outgoing data while analyzing and maintaining control of the data." —Adderson, O. G. and K. A. Wood. (2010). *A Qualitative Analysis of Strategic Capabilities for a Covert Analysis Detection System Onboard an AEGIS Class Ship*. Monterey, Calif.: Naval Postgraduate School.

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

### *Fiscal Concerns*

15. Given fiscal constraints, it is necessary to prioritize process/system implementation, upgrade, and training. Prioritize the below areas in regards to Cyber protection of ships (1—lowest priority, 5—highest priority):

| | | | | | |
|---|---|---|---|---|---|
| Offensive, e.g., Protecting against Cyber Attacks | 1 | 2 | 3 | 4 | 5 |
| Training, e.g., Cyber | 1 | 2 | 3 | 4 | 5 |
| Maintenance, e.g., Cyber Protection Infrastructure | 1 | 2 | 3 | 4 | 5 |
| Defensive, e.g., Install Cyber Protection Systems/Processes | 1 | 2 | 3 | 4 | 5 |
| Guidance, e.g., Cyber Implementation/Protection Policy | 1 | 2 | 3 | 4 | 5 |
| Other Areas of Cyber Concern: _____ | 1 | 2 | 3 | 4 | 5 |

16. Rank the below methods of implementation to increase cyber protection through systems/processes:

| | | | | | |
|---|---|---|---|---|---|
| Fleetwide | 1 | 2 | 3 | 4 | 5 |
| Deployed Platforms Only | 1 | 2 | 3 | 4 | 5 |
| Only When a Threat is Deemed Imminent | 1 | 2 | 3 | 4 | 5 |
| Platform Specific (which: _____) | 1 | 2 | 3 | 4 | 5 |
| Other Method: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Fiscal Concerns:

_____

_____

_____

### *Shipboard Network Concerns*

17. Which system is most vulnerable to cyber attack or cyber intrusion?
- ☐ Combat Systems
- ☑ Communications
- ☐ Engineering
- ☐ Navigation
- ☐ Weapons
- ☐ Other: _____

18. Which system is least vulnerable to cyber attack or cyber intrusion?
- ☐ Combat Systems
- ☐ Communications
- ☑ Engineering
- ☐ Navigation
- ☐ Weapons
- ☐ Other: _____

19. Who is usually designated to be in charge of Cyber Threat?
- ☑ Department Head
- ☐ Division Officer
- ☐ CPO
- ☐ Other: _____

20. How is this person designated?
- ☐ Primary Duty
- ☑ Collateral Duty
- ☐ Other: _____

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

21. Cyber threats can potentially affect each Department to varying degrees, rank each Department's sensitivity to such a threat (1—least, 5—most):

| | | | | | |
|---|---|---|---|---|---|
| Combat Systems | 1 | 2 | 3 | 4 | (5) |
| Operations | 1 | 2 | 3 | (4) | 5 |
| Engineering | 1 | 2 | (3) | 4 | 5 |
| Administrative | 1 | (2) | 3 | 4 | 5 |
| Weapons | (1) | 2 | 3 | 4 | 5 |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

22. Which Department should oversee Cyber protection and policy?
- ☐ Combat Systems
- ☐ Operations
- ☐ Engineering
- ☐ Administrative
- ☐ Weapons
- ☑ Other: whoever owns (owns)

23. Should the Department in charge of Cyber have a counterpart on Staff?
- ☑ Yes
- ☐ No

24. Should increased Cyber Training be given to unrestricted line (URL) Officers?
- ☑ Yes
- ☐ No

25. If yes, when should Cyber Training be given (check all that apply)?
- ☐ SWOS
- ☑ DH School
- ☑ XO/CO School
- ☐ Other: _____

Additional Comments on Shipboard Network Concerns:

_____

_____

_____

***Further Addressing Shipboard Network Concerns***

1. Rank each methods potential to help better prepare shipboard personnel for dealing with potential cyber threats (1—lowest, 5—highest):

| | | | | | |
|---|---|---|---|---|---|
| All Hands Training | 1 | 2 | 3 | 4 | (5) |
| Early Warning Detection Systems, type _____ | 1 | 2 | 3 | 4 | (5) |
| Outsourcing Systems and Maintenance | 1 | (2) | 3 | 4 | 5 |
| Schooling for Operators | 1 | 2 | 3 | (4) | 5 |
| Use of COTS | 1 | 2 | 3 | (4) | 5 |
| Covert Analysis Detection System (CADS) | 1 | 2 | 3 | 4 | (5) |
| Simulators | 1 | 2 | 3 | (4) | 5 |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

Additional Comments on Further Addressing Shipboard Network Concerns:

***Additional Information***

Additional Comments / Suggestions:

When you are done, please e-mail the survey back to me at szielech@nps.edu.

***Thank you for your participation!***

THIS PAGE INTENTIONALLY LEFT BLANK

# APPENDIX H. RESPONDENT F, DDG CO

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

## Tactics for Protecting Shipboard IT Networks

***Purpose***: Data gathered here will be used to build upon previous NPS theses that presented Covert Analysis Detection (CAD) System as a viable option for the defense of ships from cyber attacks.

***General Information***

1. Rank at time of At-Sea Command (check all that apply):
   - ☐ Lieutenant (LT)
   - ☐ Lieutenant Commander (LCDR)
   - ☒ Commander (CDR)
   - ☐ Captain (CAPT)

2. Type of ship (check all that apply):
   - ☐ Amphibious Ship, type _____
   - ☐ Cruiser (CG)
   - ☒ Destroyer (DDG)
   - ☐ Frigate (FFG)
   - ☐ Littoral Combat Ship (LCS)
   - ☐ Other, type _____

3. Weapons Department / Combat Systems Department experience:
   - ☒ Yes
   - ☐ No

4. Were any ships BMD capable?
   - ☐ Yes
   - ☒ No

5. Number of At-Sea Commands:
   - ☐ None
   - ☑ One
   - ☐ Two
   - ☐ Three
   - ☐ Four or more

***Ship Specific Concerns***

6. Rank each ship's vulnerability to cyber related attacks (1—least, 5—most):

| | | | | | |
|---|---|---|---|---|---|
| Amphibious Ship, type _____ | 1 | 2 | 3 | 4 | 5 |
| Cruiser (CG) | 1 | 2 | 3 | 4 | 5 |
| Destroyer (DDG) | 1 | 2 | 3 | 4 | 5 |
| Frigate (FFG) | 1 | 2 | 3 | 4 | 5 |
| Littoral Combat Ship (LCS) | 1 | 2 | 3 | 4 | 5 |
| Other, type _____ | 1 | 2 | 3 | 4 | 5 |

7. Which ship type is currently most vulnerable to cyber attack?
   - ☐ Amphibious Ship, type _____
   - ☒ Cruiser (CG)
   - ☒ Destroyer (DDG)
   - ☐ Frigate (FFG)
   - ☐ Littoral Combat Ship (LCS)
   - ☐ Other, type _____
   - ☒ No Difference

8. Which ship type is currently least vulnerable to cyber attack?
   - ☐ Amphibious Ship, type _____
   - ☐ Cruiser (CG)
   - ☐ Destroyer (DDG)
   - ☒ Frigate (FFG)
   - ☐ Littoral Combat Ship (LCS)
   - ☐ Other, type _____
   - ☐ No Difference

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

Additional Comments on Ship Specific Concerns:
- All ships are vulnerable to cyber attack. Some new ships have systems that make them more vulnerable

### *Cyber Threats*

9. While in Command, did you view cyber terrorism as a threat?
   - [x] Yes
   - [ ] No
10. Do you view cyber terrorism as a threat?
    - [x] Currently (within next 10 years)
    - [ ] In the future (over 10 years away)
11. When is a ship most vulnerable?
    - [ ] Homeport
    - [ ] Port Visits
    - [ ] Deployment
    - [ ] Exercises
    - [x] Other: always vulnerable
12. When is a ship least vulnerable?
    - [ ] Homeport
    - [ ] Port Visits
    - [ ] Deployment
    - [ ] Exercises
    - [x] Other: always vulnerable
13. Should ships refrain from Wi-Fi use while in port to avoid potential cyber attacks?
    - [x] N/A - Ships don't have/use not authorized Wi-Fi use
    - [ ] Yes
    - [ ] No

Additional Comments on Cyber Threats:

### *Cyber Protection Implementation & Necessity*

14. Given the potential for cyber attack, rank each method of implementing a cyber protection program/system (e.g., Covert Analysis Detection (CAD) System[1]), would be effective (1—least, 5—most):

| | | | | | |
|---|---|---|---|---|---|
| By Ship Type | 1 | 2 | 3 | 4 | 5 |
| By Numbered Fleet | 1 | 2 | 3 | 4 | 5 |
| Pre Deployment Pacakge | 1 | 2 | 3 | 4 | 5 |
| During Mid-life Upgrade | 1 | 2 | 3 | 4 | 5 |
| During Intial Building | 1 | 2 | 3 | 4 | 5 |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Cyber Protection Implementation & Necessity:
- I don't understand the question.

[1] "A CAD (Covert Analysis Detection) system is a sensor or sensor system that can covertly capture incoming and outgoing data while analyzing and maintaining control of the data." —Adderson, O. G. and K. A. Wood. (2010). *A Qualitative Analysis of Strategic Capabilities for a Covert Analysis Detection System Onboard an AEGIS Class Ship.* Monterey, Calif.: Naval Postgraduate School.

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

### *Fiscal Concerns*

15. Given fiscal constraints, it is necessary to prioritize process/system implementation, upgrade, and training. Prioritize the below areas in regards to Cyber protection of ships (1—lowest priority, 5—highest priority):

| | | | | | |
|---|---|---|---|---|---|
| Offensive, e.g., Protecting against Cyber Attacks | (1) | 2 | 3 | 4 | 5 |
| Training, e.g., Cyber | 1 | (2) | 3 | 4 | 5 |
| Maintenance, e.g., Cyber Protection Infrastructure | 1 | 2 | 3 | 4 | (5) |
| Defensive, e.g., Install Cyber Protection Systems/Processes | 1 | 2 | 3 | 4 | (5) |
| Guidance, e.g., Cyber Implementation/Protection Policy | 1 | (2) | 3 | 4 | 5 |
| Other Areas of Cyber Concern: _____ | 1 | 2 | 3 | 4 | 5 |

16. Rank the below methods of implementation to increase cyber protection through systems/processes:

| | | | | | |
|---|---|---|---|---|---|
| Fleetwide | 1 | 2 | 3 | 4 | (5) |
| Deployed Platforms Only | 1 | 2 | 3 | 4 | 5 |
| Only When a Threat is Deemed Imminent | 1 | 2 | 3 | 4 | 5 |
| Platform Specific (which: _____) | 1 | 2 | 3 | 4 | 5 |
| Other Method: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Fiscal Concerns:

_____

_____

_____

### *Shipboard Network Concerns*

17. Which system is most vulnerable to cyber attack or cyber intrusion?
- ☐ Combat Systems
- ☐ Communications
- ☐ Engineering
- ☐ Navigation
- ☐ Weapons
- ☒ Other: Information Systems

18. Which system is least vulnerable to cyber attack or cyber intrusion?
- ☐ Combat Systems
- ☐ Communications
- ☐ Engineering
- ☐ Navigation
- ☐ Weapons
- ☒ Other: Mechanical Systems

19. Who is usually designated to be in charge of Cyber Threat?
- ☐ Department Head
- ☐ Division Officer
- ☐ CPO
- ☒ Other: C 10th Fleet

20. How is this person designated?
- ☒ Primary Duty
- ☐ Collateral Duty
- ☐ Other: _____

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

21. Cyber threats can potentially affect each Department to varying degrees, rank each Department's sensitivity to such a threat (1—least, 5—most):

| | | | | | |
|---|---|---|---|---|---|
| Combat Systems | 1 | 2 | 3 | 4 | 5 |
| Operations | 1 | 2 | 3 | 4 | 5 |
| Engineering | 1 | 2 | 3 | 4 | 5 |
| Administrative | 1 | 2 | 3 | 4 | 5 |
| Weapons | 1 | 2 | 3 | 4 | 5 |
| Other: _____ What do you mean? | 1 | 2 | 3 | 4 | 5 |

22. Which Department should oversee Cyber protection and policy?
- ☐ Combat Systems
- ☐ Operations
- ☐ Engineering
- ☐ Administrative
- ☐ Weapons
- ☒ Other: _____

23. Should the Department in charge of Cyber have a counterpart on Staff?
- ☒ Yes
- ☐ No

24. Should increased Cyber Training be given to unrestricted line (URL) Officers?
- ☒ Yes
- ☐ No

25. If yes, when should Cyber Training be given (check all that apply)?
- ☐ SWOS
- ☐ DH School
- ☐ XO/CO School
- ☐ Other: _____

DH School & XO/CO School on at Shore.

Additional Comments on Shipboard Network Concerns:
- These questions are not relevant to the purpose or statement of intent of the survey

***Further Addressing Shipboard Network Concerns***

1. Rank each methods potential to help better prepare shipboard personnel for dealing with potential cyber threats (1—lowest, 5—highest):

| | | | | | |
|---|---|---|---|---|---|
| All Hands Training | 1 | 2 | 3 | 4 | 5 |
| Early Warning Detection Systems, type _____ | 1 | 2 | 3 | 4 | 5 |
| Outsourcing Systems and Maintenance | 1 | 2 | 3 | 4 | 5 |
| Schooling for Operators | 1 | 2 | 3 | 4 | 5 |
| Use of COTS | 1 | 2 | 3 | 4 | 5 |
| Covert Analysis Detection System (CADS) | 1 | 2 | 3 | 4 | 5 |
| Simulators | 1 | 2 | 3 | 4 | 5 |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

Additional Comments on Further Addressing Shipboard Network Concerns:

***Additional Information***

Additional Comments / Suggestions:

This survey should not be used in anything that resembles an academic exercise. The questions are useless for anything other than an opinion of a person in Command. This is not research.

When you are done, please e-mail the survey back to me at szielech@nps.edu.

***Thank you for your participation!***

THIS PAGE INTENTIONALLY LEFT BLANK

# APPENDIX I. RESPONDENT G, FFG CO

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

## Tactics for Protecting Shipboard IT Networks

***Purpose***: Data gathered here will be used to build upon previous NPS theses that presented Covert Analysis Detection (CAD) System as a viable option for the defense of ships from cyber attacks.

***General Information***

1. Rank at time of At-Sea Command (check all that apply):
   - ☐ Lieutenant (LT)
   - ☐ Lieutenant Commander (LCDR)
   - X Commander (CDR)
   - ☐ Captain (CAPT)

2. Type of ship (check all that apply):
   - ☐ Amphibious Ship, type _____
   - ☐ Cruiser (CG)
   - ☐ Destroyer (DDG)
   - X Frigate (FFG)
   - ☐ Littoral Combat Ship (LCS)
   - ☐ Other, type _____

3. Weapons Department / Combat Systems Department experience:
   - X Yes
   - ☐ No

4. Were any ships BMD capable?
   - ☐ Yes
   - X No

5. Number of At-Sea Commands:
   - ☐ None
   - X One
   - ☐ Two
   - ☐ Three
   - ☐ Four or more

***Ship Specific Concerns***

6. Rank each ship's vulnerability to cyber related attacks (1—least, 5—most):

| | | | | | |
|---|---|---|---|---|---|
| Amphibious Ship, type _____ | 1 | 2 | 3 | **4** | 5 |
| Cruiser (CG) | 1 | 2 | 3 | 4 | **5** |
| Destroyer (DDG) | 1 | 2 | **3** | 4 | 5 |
| Frigate (FFG) | 1 | **2** | 3 | 4 | 5 |
| Littoral Combat Ship (LCS) | **1** | 2 | 3 | 4 | 5 |
| Other, type _____ | 1 | 2 | 3 | 4 | 5 |

7. Which ship type is currently most vulnerable to cyber attack?
   - ☐ Amphibious Ship, type _____
   - ☐ Cruiser (CG)
   - ☐ Destroyer (DDG)
   - ☐ Frigate (FFG)
   - X Littoral Combat Ship (LCS)
   - ☐ Other, type _____
   - ☐ No Difference

8. Which ship type is currently least vulnerable to cyber attack?
   - ☐ Amphibious Ship, type _____
   - ☐ Cruiser (CG)
   - ☐ Destroyer (DDG)
   - ☐ Frigate (FFG)
   - ☐ Littoral Combat Ship (LCS)
   - X Other, type __CVN_____
   - ☐ No Difference

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

Additional Comments on Ship Specific Concerns:

My opinion is that the smaller the ship, less people to watch over the network in the event of an attack. Also, while in homeport, less personnel watching the network versus a deployment or exercise where the watch team is larger.

***Cyber Threats***

9. While in Command, did you view cyber terrorism as a threat?
   X Yes
   ☐ No

10. Do you view cyber terrorism as a threat?
    X Currently (within next 10 years)
    ☐ In the future (over 10 years away)

11. When is a ship most vulnerable?
    X Homeport
    ☐ Port Visits
    ☐ Deployment
    ☐ Exercises
    ☐ Other: _____

12. When is a ship least vulnerable?
    ☐ Homeport
    ☐ Port Visits
    X Deployment
    ☐ Exercises
    Other: _____

13. Should ships refrain from Wi-Fi use while in port to avoid potential cyber attacks?
    ☐ Yes
    X No-

Additional Comments on Cyber Threats:

13. WI-FI used in Mayport, FL. Not great for overall bandwidth for significant IAVA downloads.

***Cyber Protection Implementation & Necessity***

14. Given the potential for cyber attack, rank each method of implementing a cyber protection program/system (e.g., Covert Analysis Detection (CAD) System[1]), would be effective (1—least, 5—most):

| | | | | | |
|---|---|---|---|---|---|
| By Ship Type | **1** | 2 | 3 | 4 | 5 |
| By Numbered Fleet | 1 | 2 | 3 | **4** | 5 |
| Pre Deployment Package | 1 | 2 | **3** | 4 | 5 |
| During Mid-life Upgrade | 1 | **2** | 3 | 4 | 5 |
| During Intial Building | 1 | 2 | 3 | 4 | **5** |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Cyber Protection Implementation & Necessity:

Again, only an assumption on my part for this answer.

[1] "A CAD (Covert Analysis Detection) system is a sensor or sensor system that can covertly capture incoming and outgoing data while analyzing and maintaining control of the data." —Adderson, O. G. and K. A. Wood. (2010). *A Qualitative Analysis of Strategic Capabilities for a Covert Analysis Detection System Onboard an AEGIS Class Ship*. Monterey, Calif.: Naval Postgraduate School.

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

### *Fiscal Concerns*

15. Given fiscal constraints, it is necessary to prioritize process/system implementation, upgrade, and training. Prioritize the below areas in regards to Cyber protection of ships (1—lowest priority, 5—highest priority):

| | | | | | |
|---|---|---|---|---|---|
| Offensive, e.g., Protecting against Cyber Attacks | **1** | 2 | 3 | 4 | 5 |
| Training, e.g., Cyber | 1 | 2 | 3 | **4** | 5 |
| Maintenance, e.g., Cyber Protection Infrastructure | 1 | 2 | **3** | 4 | 5 |
| Defensive, e.g., Install Cyber Protection Systems/Processes | 1 | 2 | 3 | 4 | **5** |
| Guidance, e.g., Cyber Implementation/Protection Policy | 1 | **2** | 3 | 4 | 5 |
| Other Areas of Cyber Concern: _____ | 1 | 2 | 3 | 4 | 5 |

16. Rank the below methods of implementation to increase cyber protection through systems/processes:

| | | | | | |
|---|---|---|---|---|---|
| Fleetwide | 1 | 2 | 3 | 4 | **5** |
| Deployed Platforms Only | 1 | 2 | 3 | **4** | 5 |
| Only When a Threat is Deemed Imminent | **1** | 2 | **3** | 4 | 5 |
| Platform Specific (which: _____) | 1 | 2 | 3 | 4 | 5 |
| Other Method: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Fiscal Concerns:

No specific areas of concern. Even after giving a PO1 3 separate sheets of paper to review and sign as well as a discussion about USB devices, he still attempted to insert a USB device- the internal threat remains a concern.

### *Shipboard Network Concerns*

17. Which system is most vulnerable to cyber attack or cyber intrusion?
- ☐ Combat Systems
- X Communications
- ☐ Engineering
- ☐ Navigation
- ☐ Weapons
- ☐ Other: _____

18. Which system is least vulnerable to cyber attack or cyber intrusion?
- ☐ Combat Systems
- ☐ Communications
- X Engineering
- ☐ Navigation
- ☐ Weapons
- ☐ Other: _____

19. Who is usually designated to be in charge of Cyber Threat?
- ☐ Department Head
- ☐ Division Officer
- X CPO
- ☐ Other: _____

20. How is this person designated?
- X Primary Duty
- ☐ Collateral Duty
- ☐ Other: _____

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

21. Cyber threats can potentially affect each Department to varying degrees, rank each Department's sensitivity to such a threat (1—least, 5—most):

| | | | | | |
|---|---|---|---|---|---|
| Combat Systems | 1 | 2 | **3** | 4 | 5 |
| Operations | 1 | 2 | 3 | 4 | **5** |
| Engineering | **1** | 2 | 3 | 4 | 5 |
| Administrative | 1 | 2 | 3 | **4** | 5 |
| Weapons | 1 | **2** | 3 | 4 | 5 |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

22. Which Department should oversee Cyber protection and policy?
- ☐ Combat Systems
- X Operations
- ☐ Engineering
- ☐ Administrative
- ☐ Weapons
- ☐ Other: _____

23. Should the Department in charge of Cyber have a counterpart on Staff?
- X Yes
- ☐ No

24. Should increased Cyber Training be given to unrestricted line (URL) Officers?
- X Yes
- ☐ No

25. If yes, when should Cyber Training be given (check all that apply)?
- X SWOS
- ☐ DH School
- ☐ XO/CO School
- ☐ Other: _____

Additional Comments on Shipboard Network Concerns:

_____

_____

_____

***Further Addressing Shipboard Network Concerns***

1. Rank each methods potential to help better prepare shipboard personnel for dealing with potential cyber threats (1—lowest, 5—highest):

| | | | | | |
|---|---|---|---|---|---|
| All Hands Training | **1** | 2 | 3 | 4 | 5 |
| Early Warning Detection Systems, type _____ | 1 | **2** | 3 | 4 | 5 |
| Outsourcing Systems and Maintenance | 1 | 2 | 3 | 4 | 5 |
| Schooling for Operators | 1 | 2 | 3 | 4 | **5** |
| Use of COTS | 1 | 2 | 3 | 4 | 5 |
| Covert Analysis Detection System (CADS) | 1 | 2 | 3 | **4** | 5 |
| Simulators | 1 | 2 | **3** | 4 | 5 |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

Additional Comments on Further Addressing Shipboard Network Concerns:

_____

_____

_____

***Additional Information***

Additional Comments / Suggestions:

Good luck on your study. Not sure that my input supports your needs, but wish you the best with it.

_____

_____

_____

When you are done, please e-mail the survey back to me at szielech@nps.edu.

***Thank you for your participation!***

THIS PAGE INTENTIONALLY LEFT BLANK

# APPENDIX J. RESPONDENT H, CG CO

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

## Tactics for Protecting Shipboard IT Networks

***Purpose***: Data gathered here will be used to build upon previous NPS theses that presented Covert Analysis Detection (CAD) System as a viable option for the defense of ships from cyber attacks.

***General Information***

1. Rank(s) at time of At-Sea Command (check all that apply):
   - ☐ Lieutenant (LT)
   - ☐ Lieutenant Commander (LCDR)
   - ☐ xCommander (CDR)
   - ☐ xCaptain (CAPT)
2. Number of At-Sea Commands:
   - ☐ None
   - ☐ One
   - ☐ xTwo
   - ☐ Three
   - ☐ Four or more
3. Were you ever a Weapons or a Combat Systems Department Head?
   - ☐ xYes
   - ☐ No
4. Were any of your ships Ballistic Missile Defense (BMD) capable?
   - ☐ Yes
   - ☐ xNo
5. Type of ship(s) (check all that apply):
   - ☐ Aircraft Carrier (CVN)
   - ☐ Amphibious Ship (LHA/LHD, LCC, LPD, or LSD), type _____
   - ☐ xCruiser (CG)
   - ☐ xDestroyer (DDG)
   - ☐ xFrigate (FFG)
   - ☐ Littoral Combat Ship (LCS)
   - ☐ Mine Countermeasures Ship (MCM)
   - ☐ Patrol Coastal Ship (PC)
   - ☐ Other, type _____

***Ship Specific Concerns***

6. Individually rate each ships' overall vulnerability to a cyber related attack (1—lowest, 2—low, 3—average, 4—high, 5—highest):

| | | | | | |
|---|---|---|---|---|---|
| Aircraft Carrier (CVN) | 1 | 2 | 3 | 4 | 5 |
| Amphibious Ship (LHA/LHD, LCC, LPD, or LSD), type _____ | 1 | 2 | 3 | 4 | 5 |
| Cruiser (CG) | 1 | 2 | 3 | 4x | 5 |
| Destroyer (DDG) | 1 | 2 | 3 | 4 | 5x |
| Frigate (FFG) | 1 | 2 | 3 | 4 | 5x |
| Littoral Combat Ship (LCS) | 1 | 2 | 3 | 4 | 5 |
| Mine Countermeasures Ship (MCM) | 1 | 2 | 3 | 4 | 5 |
| Patrol Coastal Ship (PC) | 1 | 2 | 3 | 4 | 5 |
| Other, type _____ | 1 | 2 | 3 | 4 | 5 |

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

7. Overall, which ship type is currently the *most* vulnerable to a cyber attack?
   - ☐ Aircraft Carrier (CVN)
   - ☐ Amphibious Ship (LHA/LHD, LCC, LPD, or LSD), type _____
   - ☐ Cruiser (CG)
   - ☐ xDestroyer (DDG)
   - ☐ xFrigate (FFG)
   - ☐ Littoral Combat Ship (LCS)
   - ☐ Mine Countermeasures Ship (MCM)
   - ☐ Patrol Coastal Ship (PC)
   - ☐ Other, type _____

8. Overall, which ship type is currently the *least* vulnerable to a cyber attack?
   - ☐ Aircraft Carrier (CVN)
   - ☐ Amphibious Ship (LHA/LHD, LCC, LPD, or LSD), type _____
   - ☐ xCruiser (CG)
   - ☐ Destroyer (DDG)
   - ☐ Frigate (FFG)
   - ☐ Littoral Combat Ship (LCS)
   - ☐ Mine Countermeasures Ship (MCM)
   - ☐ Patrol Coastal Ship (PC)
   - ☐ Other, type _____

Additional Comments on Ship Specific Concerns:

_____
_____
_____

***Cyber Threats***

9. While in Command, did you view cyber terrorism as a threat?
   - ☐ Yes
   - ☐ xNo

10. Cyber Terrorism is a _____ threat.
    - ☐ xCurrent (within next 10 years)
    - ☐ Future (over 10 years away)

11. When is a ship *most* vulnerable?
    - ☐ Homeport
    - ☐ Port Visits
    - ☐ xDeployment
    - ☐ Exercises
    - ☐ Other: _____

12. When is a ship *least* vulnerable?
    - ☐ Homeport
    - ☐ Port Visits
    - ☐ Deployment
    - ☐ xExercises
    - Other: _____

13. Should ships refrain from Wi-Fi use while in port to avoid potential cyber attacks?
    - ☐ Yes
    - ☐ xNo

Additional Comments on Cyber Threats:

_____
_____
_____

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

### *Cyber Protection Implementation & Necessity*

14. Given the potential for a cyber attack, rank the effectiveness of each implementation approach for cyber protection programs/systems, e.g., installing Covert Analysis Detection (CAD) System[1], (1—least effective, 2—less effective, 3—effective, 4—more effective, 5—most effective):

| | | | | | |
|---|---|---|---|---|---|
| By Ship Type | 1 | 2 | 3 | 4 | 5 |
| By Numbered Fleet | 1 | 2 | 3 | 4 | 5 |
| Pre-deployment Package | 1 | 2 | 3 | x4 | 5 |
| During Mid-life Upgrade | 1 | 2 | x3 | 4 | 5 |
| During Intial Shipbuilding | 1 | 2 | 3 | 4 | x5 |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Cyber Protection Implementation & Necessity:

_____

_____

_____

### *Fiscal Concerns*

15. Given current and expected future fiscal constraints, it is necessary to prioritize the needs of a ship. Rank the below areas of shipboard Cyber protection (1—lowest priority, 2—lower priority, 3—priority, 4—higher priority, 5—highest priority):

| | | | | | |
|---|---|---|---|---|---|
| Defensive, e.g., Install Cyber Protection Systems/Processes | 1 | 2 | 3 | x4 | 5 |
| Guidance, e.g., Cyber Implementation/Protection Policy | 1 | 2 | 3 | x4 | 5 |
| Maintenance, e.g., Cyber Protection Infrastructure | 1 | x2 | 3 | 4 | 5 |
| Offensive, e.g., Protecting against Cyber Attacks | 1 | 2 | x3 | 4 | 5 |
| Training, e.g., Cyber | 1 | 2 | x3 | 4 | 5 |
| Other Areas of Cyber Concern: _____ | 1 | 2 | 3 | 4 | 5 |

[1] "A CAD (Covert Analysis Detection) system is a sensor or sensor system that can covertly capture incoming and outgoing data while analyzing and maintaining control of the data." —Adderson, O. G. and K. A. Wood. (2010). *A Qualitative Analysis of Strategic Capabilities for a Covert Analysis Detection System Onboard an AEGIS Class Ship*. Monterey, Calif.: Naval Postgraduate School.

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

16. Given current and expected future fiscal constraints, rank the below approaches to the implementation of processes/systems to increase cyber security on ships (1—worst approach, 2—worse approach, 3—acceptable approach, 4—better approach, 5—best approach):

| | | | | | |
|---|---|---|---|---|---|
| Fleetwide | 1 | 2 | 3 | 4 | 5 |
| Deployed Platforms Only | 1 | 2 | 3 | 4 | 5 |
| Only When a Threat is Deemed Imminent | 1 | 2 | 3 | x4 | 5 |
| Platform Specific (which: _____) | 1 | 2 | 3 | 4 | 5 |
| During Initial Shipbuilding | 1 | 2 | 3 | 4 | x5 |
| Other Method: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Fiscal Concerns:

_____

_____

_____

***Shipboard Network Concerns***

17. Which shipboard system is *most critical* during a time of conflict, i.e., must remain online throughout to defend the ship or other assets in the AOR?
    - ☐ xCombat Systems
    - ☐ Communications
    - ☐ Engineering
    - ☐ Navigation
    - ☐ Weapons
    - ☐ Other: _____

18. Which shipboard system is *least critical* during a time of conflict?
    - ☐ Combat Systems
    - ☐ Communications
    - ☐ Engineering
    - ☐ xNavigation
    - ☐ Weapons
    - ☐ Other: _____

19. Who is usually designated to be in charge of Cyber issues aboard ship, e.g., training, instructions, protection measures?
    - ☐ Department Head
    - ☐ Division Officer
    - ☐ CPO
    - ☐ Other: don't know_____

20. How is this person designated?
    - ☐ Primary Duty
    - ☐ Collateral Duty
    - ☐ Other: don't know_____

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

21. Cyber threats can potentially affect each Department to varying degrees, rank the following Departments according to their overall sensitivity to such a threat (1—least sensitive, 2—less sensitive, 3—sensitive, 4—more sensitive, 5—most sensitive):

| | | | | | |
|---|---|---|---|---|---|
| Administrative | x1 | 2 | 3 | 4 | 5 |
| Combat Systems | 1 | 2 | 3 | 4 | x5 |
| Engineering | 1 | 2 | x3 | 4 | 5 |
| Operations | 1 | 2 | 3 | x4 | 5 |
| Weapons | 1 | 2 | 3 | x4 | 5 |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

22. Which Department should oversee Cyber issues, including protection, policy, training, etc.?
- ☐ Administrative
- ☐ xCombat Systems
- ☐ Engineering
- ☐ Operations
- ☐ Weapons
- ☐ Other: _____

23. Should the Department in charge of Cyber have a counterpart on Staff?
- ☐ xYes
- ☐ No

24. Should more Cyber Training be given to unrestricted line (URL) Officers?
- ☐ xYes
- ☐ No

25. If yes, when should Cyber Training be given (check all that apply)?
- ☐ xBasic Division Officer Course
- ☐ DH School
- ☐ XO/CO School
- ☐ Other: _____

Additional Comments on Shipboard Network Concerns:

_____

_____

_____

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

***Further Addressing Shipboard Network Concerns***

26. Rate each methods' potential to improve a crew's ability to deal with cyber threats (1—lowest potential, 2—lower potential, 3—average potential, 4—higher potential, 5—highest potential):

| | | | | | |
|---|---|---|---|---|---|
| All Hands Training | 1 | 2 | x3 | 4 | 5 |
| Early Warning Detection Systems, type _____ | 1 | 2 | x3 | 4 | 5 |
| Outsourcing Systems and Maintenance | 1 | x2 | 3 | 4 | 5 |
| Schooling for Operators | 1 | 2 | x3 | 4 | 5 |
| Use of Commercial Off-The-Shelf (COTS) Systems | 1 | x2 | 3 | 4 | 5 |
| Covert Analysis Detection System (CADS) | 1 | 2 | 3 | x4 | 5 |
| Simulators | 1 | 2 | x3 | 4 | 5 |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Further Addressing Shipboard Network Concerns:

_____

_____

_____

***Additional Information***

Additional Comments / Suggestions:

I'm a dinosaur. Cyber warfare didn't exist when I was in command, so you may consider this an uniformed response

_____

_____

_____

When you are done, please e-mail the survey back to me at szielech@nps.edu.

***Thank you for your participation!***

# APPENDIX K. RESPONDENT I, CG CO

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

## Tactics for Protecting Shipboard IT Networks

***Purpose***: Data gathered here will be used to build upon previous NPS theses that presented Covert Analysis Detection (CAD) System as a viable option for the defense of ships from cyber attacks.

***General Information***

1. Rank(s) at time of At-Sea Command (check all that apply):
   - ☐ Lieutenant (LT)
   - ☐ Lieutenant Commander (LCDR)
   - ☐ Commander (CDR)
   - X Captain (CAPT)
2. Number of At-Sea Commands:
   - ☐ None
   - ☐ One
   - X Two
   - ☐ Three
   - ☐ Four or more
3. Were you ever a Weapons or a Combat Systems Department Head?
   - X Yes
   - ☐ No
4. Were any of your ships Ballistic Missile Defense (BMD) capable?
   - ☐ Yes
   - X No (as a DESRON Commander, I had 4 BMD capable ships)
5. Type of ship(s) (check all that apply):
   - X Aircraft Carrier (CVN)
   - X Amphibious Ship (LHA/LHD, LCC, LPD, or LSD), type _____
   - X Cruiser (CG)
   - X Destroyer (DDG)
   - ☐ Frigate (FFG)
   - ☐ Littoral Combat Ship (LCS)
   - ☐ Mine Countermeasures Ship (MCM)
   - X Patrol Coastal Ship (PC)
   - ☐ Other, type _____

***Ship Specific Concerns***

6. Individually rate each ships' overall vulnerability to a cyber related attack (1—lowest, 2—low, 3—average, 4—high, 5—highest):

| | | | | | |
|---|---|---|---|---|---|
| Aircraft Carrier (CVN) | 1 | 2 | 3 | 4 | (5) |
| Amphibious Ship (LHA/LHD, LCC, LPD, or LSD), type _____ | 1 | 2 | 3 | 4 | (5) |
| Cruiser (CG) | 1 | 2 | 3 | 4 | (5) |
| Destroyer (DDG) | 1 | 2 | 3 | 4 | (5) |
| Frigate (FFG) | 1 | 2 | 3 | 4 | (5) |
| Littoral Combat Ship (LCS) | 1 | 2 | 3 | 4 | (5) |
| Mine Countermeasures Ship (MCM) | 1 | 2 | 3 | 4 | (5) |
| Patrol Coastal Ship (PC) | 1 | 2 | 3 | 4 | (5) |
| Other, type _____ | 1 | 2 | 3 | 4 | (5) |

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

7. Overall, which ship type is currently the *most* vulnerable to a cyber attack?
   - X Aircraft Carrier (CVN)
   - ☐ Amphibious Ship (LHA/LHD, LCC, LPD, or LSD), type _____
   - ☐ Cruiser (CG)
   - ☐ Destroyer (DDG)
   - ☐ Frigate (FFG)
   - ☐ Littoral Combat Ship (LCS)
   - ☐ Mine Countermeasures Ship (MCM)
   - ☐ Patrol Coastal Ship (PC)
   - ☐ Other, type _____

8. Overall, which ship type is currently the *least* vulnerable to a cyber attack?
   - ☐ Aircraft Carrier (CVN)
   - ☐ Amphibious Ship (LHA/LHD, LCC, LPD, or LSD), type _____
   - ☐ Cruiser (CG)
   - ☐ Destroyer (DDG)
   - ☐ Frigate (FFG)
   - X Littoral Combat Ship (LCS)
   - X Mine Countermeasures Ship (MCM)
   - X Patrol Coastal Ship (PC)
   - ☐ Other, type _____

Additional Comments on Ship Specific Concerns:

CVNs have the most C4I networks and are more vulnerable. The less C4I a ship has the less vulnerable they are to cyber attacks.

***Cyber Threats***

9. While in Command, did you view cyber terrorism as a threat?
   - X Yes
   - ☐ No

10. Cyber Terrorism is a _____ threat.
    - X Current (within next 10 years)
    - ☐ Future (over 10 years away)

11. When is a ship *most* vulnerable?
    - ☐ Homeport
    - ☐ Port Visits
    - ☐ Deployment
    - ☐ Exercises
    - X Other: ___ALL the time_____

12. When is a ship *least* vulnerable?
    - ☐ Homeport
    - ☐ Port Visits
    - ☐ Deployment
    - ☐ Exercises
    - X Other: Never or when their system is not operational

13. Should ships refrain from Wi-Fi use while in port to avoid potential cyber attacks?
    - X Yes
    - ☐ No

Additional Comments on Cyber Threats:

The increase in smart phones and video games has increased the level of vulnerability. I would submit that when a ship is operating in a choke point or strait transit, they are just if not more vulnerable to a cyber-attack which would reduce their combat effectiveness.

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

***Cyber Protection Implementation & Necessity***

14. Given the potential for a cyber attack, rank the effectiveness of each implementation approach for cyber protection programs/systems, e.g., installing Covert Analysis Detection (CAD) System[1], (1—least effective, 2—less effective, 3—effective, 4—more effective, 5—most effective):

| | | | | | |
|---|---|---|---|---|---|
| By Ship Type | 1 | 2 | (3) | 4 | 5 |
| By Numbered Fleet | 1 | 2 | (3) | 4 | 5 |
| Pre-deployment Package | 1 | 2 | 3 | (4) | 5 |
| During Mid-life Upgrade | 1 | 2 | 3 | 4 | (5) |
| During Intial Shipbuilding | 1 | 2 | 3 | 4 | (5) |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Cyber Protection Implementation & Necessity:

_____

_____

_____

***Fiscal Concerns***

15. Given current and expected future fiscal constraints, it is necessary to prioritize the needs of a ship. Rank the below areas of shipboard Cyber protection (1—lowest priority, 2—lower priority, 3—priority, 4—higher priority, 5—highest priority):

| | | | | | |
|---|---|---|---|---|---|
| Defensive, e.g., Install Cyber Protection Systems/Processes | 1 | 2 | 3 | 4 | (5) |
| Guidance, e.g., Cyber Implementation/Protection Policy | 1 | 2 | 3 | (4) | 5 |
| Maintenance, e.g., Cyber Protection Infrastructure | 1 | 2 | 3 | 4 | (5) |
| Offensive, e.g., Protecting against Cyber Attacks | 1 | 2 | (3) | 4 | 5 |
| Training, e.g., Cyber | 1 | 2 | 3 | 4 | (5) |
| Other Areas of Cyber Concern: _____ | 1 | 2 | 3 | 4 | 5 |

[1] "A CAD (Covert Analysis Detection) system is a sensor or sensor system that can covertly capture incoming and outgoing data while analyzing and maintaining control of the data." —Adderson, O. G. and K. A. Wood. (2010). *A Qualitative Analysis of Strategic Capabilities for a Covert Analysis Detection System Onboard an AEGIS Class Ship*. Monterey, Calif.: Naval Postgraduate School.

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

16. Given current and expected future fiscal constraints, rank the below approaches to the implementation of processes/systems to increase cyber security on ships (1—worst approach, 2—worse approach, 3—acceptable approach, 4—better approach, 5--best approach):

| | | | | | |
|---|---|---|---|---|---|
| Fleetwide | 1 | (2) | 3 | 4 | 5 |
| Deployed Platforms Only | 1 | 2 | 3 | 4 | (5) |
| Only When a Threat is Deemed Imminent | 1 | (2) | 3 | 4 | 5 |
| Platform Specific (which: _____) | 1 | 2 | 3 | 4 | 5 |
| During Initial Shipbuilding | 1 | (2) | 3 | 4 | 5 |
| Other Method: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Fiscal Concerns:

_____

_____

_____

***Shipboard Network Concerns***

17. Which shipboard system is *most critical* during a time of conflict, i.e., must remain online throughout to defend the ship or other assets in the AOR?
- X Combat Systems
- ☐ Communications
- ☐ Engineering
- ☐ Navigation
- ☐ Weapons
- ☐ Other: _____

18. Which shipboard system is *least critical* during a time of conflict?
- ☐ Combat Systems
- ☐ Communications
- ☐ Engineering
- ☐ Navigation
- ☐ Weapons
- X Other: Admin and Supply systems

19. Who is usually designated to be in charge of Cyber issues aboard ship, e.g., training, instructions, protection measures?
- ☐ Department Head
- ☐ Division Officer
- X CPO
- ☐ Other: _____

20. How is this person designated?
- ☐ Primary Duty
- X Collateral Duty
- ☐ Other: _____

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

21. Cyber threats can potentially affect each Department to varying degrees, rank the following Departments according to their overall sensitivity to such a threat (1—least sensitive, 2—less sensitive, 3—sensitive, 4—more sensitive, 5—most sensitive):

| | | | | | |
|---|---|---|---|---|---|
| Administrative | (1) | 2 | 3 | 4 | 5 |
| Combat Systems | 1 | 2 | 3 | 4 | (5) |
| Engineering | 1 | 2 | 3 | (4) | 5 |
| Operations | 1 | 2 | 3 | 4 | (5) |
| Weapons | 1 | 2 | 3 | 4 | (5) |
| Other: _____Communications is vital | 1 | 2 | 3 | 4 | (5) |

22. Which Department should oversee Cyber issues, including protection, policy, training, etc.?
- ☐ Administrative
- X Combat Systems
- ☐ Engineering
- ☐ Operations
- ☐ Weapons
- ☐ Other: _____

23. Should the Department in charge of Cyber have a counterpart on Staff?
- X Yes
- ☐ No

24. Should more Cyber Training be given to unrestricted line (URL) Officers?
- X Yes
- ☐ No

25. If yes, when should Cyber Training be given (check all that apply)?
- ☐ Basic Division Officer Course
- ☐ DH School
- ☐ XO/CO School
- X Other: At ALL levels

Additional Comments on Shipboard Network Concerns:

_____
_____
_____

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

***Further Addressing Shipboard Network Concerns***

26. Rate each methods' potential to improve a crew's ability to deal with cyber threats (1—lowest potential, 2—lower potential, 3—average potential, 4—higher potential, 5—highest potential):

| | | | | | |
|---|---|---|---|---|---|
| All Hands Training | 1 | 2 | 3 | 4 | (5) |
| Early Warning Detection Systems, type _____ | 1 | 2 | (3) | 4 | 5 |
| Outsourcing Systems and Maintenance | 1 | (2) | 3 | 4 | 5 |
| Schooling for Operators | 1 | 2 | 3 | 4 | (5) |
| Use of Commercial Off-The-Shelf (COTS) Systems | 1 | 2 | 3 | 4 | (5) |
| Covert Analysis Detection System (CADS) | 1 | 2 | (3) | 4 | 5 |
| Simulators | 1 | (2) | 3 | 4 | 5 |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Further Addressing Shipboard Network Concerns:

_____

_____

_____

***Additional Information***

Additional Comments / Suggestions:

_____

_____

_____

_____

When you are done, please e-mail the survey back to me at szielech@nps.edu.

***Thank you for your participation!***

# APPENDIX L. RESPONDENT J, MCM CO

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

## Tactics for Protecting Shipboard IT Networks

***Purpose***: Data gathered here will be used to build upon previous NPS theses that presented Covert Analysis Detection (CAD) System as a viable option for the defense of ships from cyber attacks.

***General Information***

1. Rank(s) at time of At-Sea Command (check all that apply):
   - ☐ Lieutenant (LT)
   - X Lieutenant Commander (LCDR)
   - ☐ Commander (CDR)
   - ☐ Captain (CAPT)
2. Number of At-Sea Commands:
   - ☐ None
   - X One
   - ☐ Two
   - ☐ Three
   - ☐ Four or more
3. Were you ever a Weapons or a Combat Systems Department Head?
   - ☐ Yes
   - X No
4. Were any of your ships Ballistic Missile Defense (BMD) capable?
   - ☐ Yes
   - X No
5. Type of ship(s) (check all that apply):
   - ☐ Aircraft Carrier (CVN)
   - ☐ Amphibious Ship (LHA/LHD, LCC, LPD, or LSD), type _____
   - ☐ Cruiser (CG)
   - ☐ Destroyer (DDG)
   - ☐ Frigate (FFG)
   - ☐ Littoral Combat Ship (LCS)
   - X Mine Countermeasures Ship (MCM)
   - ☐ Patrol Coastal Ship (PC)
   - ☐ Other, type _____

***Ship Specific Concerns***

6. Individually rate each ships' overall vulnerability to a cyber related attack (1—lowest, 2—low, 3—average, 4—high, 5—highest):

| | | | | | |
|---|---|---|---|---|---|
| Aircraft Carrier (CVN) | 1 | 2 | 3 | | 5 |
| Amphibious Ship (LHA/LHD, LCC, LPD, or LSD), type _____ | 1 | 2 | | 4 | 5 |
| Cruiser (CG) | 1 | 2 | 3 | | 5 |
| Destroyer (DDG) | 1 | 2 | 3 | | 5 |
| Frigate (FFG) | 1 | | 3 | 4 | 5 |
| Littoral Combat Ship (LCS) | 1 | 2 | | 4 | 5 |
| Mine Countermeasures Ship (MCM) | 1 | | 3 | 4 | 5 |
| Patrol Coastal Ship (PC) | 1 | | 3 | 4 | 5 |
| Other, type _____ | 1 | 2 | 3 | 4 | 5 |

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

7. Overall, which ship type is currently the *most* vulnerable to a cyber attack?
   - ☐ Aircraft Carrier (CVN)
   - ☐ Amphibious Ship (LHA/LHD, LCC, LPD, or LSD), type _____
   - X Cruiser (CG)
   - ☐ Destroyer (DDG)
   - ☐ Frigate (FFG)
   - ☐ Littoral Combat Ship (LCS)
   - ☐ Mine Countermeasures Ship (MCM)
   - ☐ Patrol Coastal Ship (PC)
   - ☐ Other, type _____

8. Overall, which ship type is currently the *least* vulnerable to a cyber attack?
   - ☐ Aircraft Carrier (CVN)
   - ☐ Amphibious Ship (LHA/LHD, LCC, LPD, or LSD), type _____
   - ☐ Cruiser (CG)
   - ☐ Destroyer (DDG)
   - ☐ Frigate (FFG)
   - ☐ Littoral Combat Ship (LCS)
   - X Mine Countermeasures Ship (MCM)
   - ☐ Patrol Coastal Ship (PC)
   - ☐ Other, type _____

Additional Comments on Ship Specific Concerns:

Overall there is little threat to the systems on either an MCM, FFG or PC due to the lack of integrated systems that require dedicated connected network access.

***Cyber Threats***

9. While in Command, did you view cyber terrorism as a threat?
   - ☐ Yes
   - X No

10. Cyber Terrorism is a _____ threat.
    - ☐ Current (within next 10 years)
    - X Future (over 10 years away)

11. When is a ship *most* vulnerable?
    - X Homeport
    - ☐ Port Visits
    - ☐ Deployment
    - ☐ Exercises
    - ☐ Other: _____

12. When is a ship *least* vulnerable?
    - ☐ Homeport
    - ☐ Port Visits
    - X Deployment
    - ☐ Exercises
    - Other: _____

13. Should ships refrain from Wi-Fi use while in port to avoid potential cyber attacks?
    - ☐ Yes
    - X No

Additional Comments on Cyber Threats:

The only Wi-FI use I have seen onboard ships has been on a separate (MWR) network than shipboard LAN, which is relatively low risk for threat to naval systems.

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

***Cyber Protection Implementation & Necessity***

14. Given the potential for a cyber attack, rank the effectiveness of each implementation approach for cyber protection programs/systems, e.g., installing Covert Analysis Detection (CAD) System[1], (1—least effective, 2—less effective, 3—effective, 4—more effective, 5—most effective):

| | | | | | |
|---|---|---|---|---|---|
| By Ship Type | 1 | 2 | 3 | 4 | |
| By Numbered Fleet | 1 | 2 | | 4 | 5 |
| Pre-deployment Package | 1 | | 3 | 4 | 5 |
| During Mid-life Upgrade | 1 | 2 | 3 | 4 | |
| During Intial Shipbuilding | | 2 | 3 | 4 | 5 |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Cyber Protection Implementation & Necessity:

Implementation should be completed in a phased method with the ability to push updates to ships, vice reliance on shipboard personnel to update manually. I'm not sure I understand the necessity of the system.

***Fiscal Concerns***

15. Given current and expected future fiscal constraints, it is necessary to prioritize the needs of a ship. Rank the below areas of shipboard Cyber protection (1—lowest priority, 2—lower priority, 3—priority, 4—higher priority, 5—highest priority):

| | | | | | |
|---|---|---|---|---|---|
| Defensive, e.g., Install Cyber Protection Systems/Processes | 1 | 2 | 3 | | 5 |
| Guidance, e.g., Cyber Implementation/Protection Policy | 1 | | 3 | 4 | 5 |
| Maintenance, e.g., Cyber Protection Infrastructure | 1 | 2 | 3 | 4 | |
| Offensive, e.g., Protecting against Cyber Attacks | 1 | | 3 | 4 | 5 |
| Training, e.g., Cyber | 1 | 2 | 3 | 4 | |
| Other Areas of Cyber Concern: _____ | 1 | 2 | 3 | 4 | 5 |

[1] "A CAD (Covert Analysis Detection) system is a sensor or sensor system that can covertly capture incoming and outgoing data while analyzing and maintaining control of the data." —Adderson, O. G. and K. A. Wood. (2010). *A Qualitative Analysis of Strategic Capabilities for a Covert Analysis Detection System Onboard an AEGIS Class Ship*. Monterey, Calif.: Naval Postgraduate School.

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

16. Given current and expected future fiscal constraints, rank the below approaches to the implementation of processes/systems to increase cyber security on ships (1—worst approach, 2—worse approach, 3—acceptable approach, 4—better approach, 5—best approach):

| | | | | | |
|---|---|---|---|---|---|
| Fleetwide | 1 | | 3 | 4 | 5 |
| Deployed Platforms Only | 1 | 2 | 3 | | 5 |
| Only When a Threat is Deemed Imminent | | 2 | 3 | 4 | 5 |
| Platform Specific (which: CG/DDG) | 1 | 2 | | 4 | 5 |
| During Initial Shipbuilding | 1 | 2 | | 4 | 5 |
| Other Method: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Fiscal Concerns:

The current cyber security approach requires administrators to "pull" the patches and creates constant headaches regarding reporting and compliance. The systems should be "pushed" to the fleet with additional support to correct discrepancies. Much of the current cyber security requirements also are weighed heavily towards denial and restriction, vice how the security increases or decreases productivity or affects overall system function.

***Shipboard Network Concerns***

17. Which shipboard system is *most critical* during a time of conflict, i.e., must remain online throughout to defend the ship or other assets in the AOR?
    - ☐ Combat Systems
    - X Communications
    - ☐ Engineering
    - ☐ Navigation
    - ☐ Weapons
    - ☐ Other: _____

18. Which shipboard system is *least critical* during a time of conflict?
    - ☐ Combat Systems
    - ☐ Communications
    - ☐ Engineering
    - ☐ Navigation
    - ☐ Weapons
    - X Other: _Admin (NIAPS)____

19. Who is usually designated to be in charge of Cyber issues aboard ship, e.g., training, instructions, protection measures?
    - ☐ Department Head
    - X Division Officer
    - ☐ CPO
    - ☐ Other: _____

20. How is this person designated?
    - ☐ Primary Duty
    - X Collateral Duty
    - ☐ Other: _____

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

21. Cyber threats can potentially affect each Department to varying degrees, rank the following Departments according to their overall sensitivity to such a threat (1—least sensitive, 2—less sensitive, 3—sensitive, 4—more sensitive, 5—most sensitive):

| | | | | | |
|---|---|---|---|---|---|
| Administrative | | 2 | 3 | 4 | 5 |
| Combat Systems | 1 | 2 | 3 | | 5 |
| Engineering | 1 | 2 | 3 | | 5 |
| Operations | 1 | | 3 | 4 | 5 |
| Weapons | 1 | 2 | 3 | 4 | |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

22. Which Department should oversee Cyber issues, including protection, policy, training, etc.?
- ☐ Administrative
- X Combat Systems
- ☐ Engineering
- ☐ Operations
- ☐ Weapons
- ☐ Other: _____

23. Should the Department in charge of Cyber have a counterpart on Staff?
- ☐ Yes
- X No

24. Should more Cyber Training be given to unrestricted line (URL) Officers?
- X Yes
- ☐ No

25. If yes, when should Cyber Training be given (check all that apply)?
- X Basic Division Officer Course
- ☐ DH School
- X XO/CO School
- ☐ Other: _____

Additional Comments on Shipboard Network Concerns:

Although I have seen a few videos that demonstrate the capabilities of some of the cyber-threats, the vulnerability of shipboard systems is significantly less than the shore-side concerns.

LT Steven Zielechowski
szielech@nps.edu
(724) 812-3870

***Further Addressing Shipboard Network Concerns***

26. Rate each methods' potential to improve a crew's ability to deal with cyber threats (1—lowest potential, 2—lower potential, 3—average potential, 4—higher potential, 5—highest potential):

| | | | | | |
|---|---|---|---|---|---|
| All Hands Training | | 2 | 3 | 4 | 5 |
| Early Warning Detection Systems, type _____ | 1 | 2 | | 4 | 5 |
| Outsourcing Systems and Maintenance | | 2 | 3 | 4 | 5 |
| Schooling for Operators | 1 | 2 | 3 | 4 | |
| Use of Commercial Off-The-Shelf (COTS) Systems | 1 | 2 | 3 | | 5 |
| Covert Analysis Detection System (CADS) | 1 | 2 | | 4 | 5 |
| Simulators | | 2 | 3 | 4 | 5 |
| Other: _____ | 1 | 2 | 3 | 4 | 5 |

Additional Comments on Further Addressing Shipboard Network Concerns:

_____

_____

_____

***Additional Information***

Additional Comments / Suggestions:

If there is a greater desire to protect our shipboard networks, there has to be a greater push on the overall force towards cyber threats and vulnerabilities. For the most part, the only training most Sailors receive is the annual IA compliance NKO. Ships are greatly undermanned in trained personnel to deal with shipboard networks (1-2 per ship is average) and already overloaded by the current workload. If there is a way to "push" additional protections to the ships, vice requiring additional training and time to implement the patches, it would go a long way towards decreasing network vulnerabilities.

When you are done, please e-mail the survey back to me at szielech@nps.edu.

***Thank you for your participation!***

# LIST OF REFERENCES


Adderson, Orenthal G. and Kristy A. Wood. "A Qualitative Analysis of Strategic Capabilities for a Covert Analysis Detection System Onboard an AEGIS Class Ship." Master's thesis, Naval Postgraduate School, 2010.

Andrews, Sean M. "Optimizing C4ISR Networks in the Presence of Enemy Jamming." Master's thesis, Naval Postgraduate School, 2010.

Brown, Michael A. "Navy Operations to Achieve Military Power in Cyberspace: A Draft Concept for Navy Computer Operations," *Military Perspectives on Cyberpower*, edited by Larry K. Wendt, Charles L. Barry, and Stuart H. Starr. Washington, DC: National Defense University, 2009.

Center for Naval Analysis. "The Navy Role in Confronting Irregular Challenges Implementing the Navy Vision for CIC." March 2011. Accessed March 28, 2014, http://www.cna.org/sites/default/files/research/The%20Navy%20Role%20in%20Confronting%20Irregular%20Challenges.pdf

Clarke, Richard A. and Robert Knake. *Cyber War: The Next Threat to National Security*. New York: HarperCollins Publishers, 2010.

Committee on Information Assurance for Network-Centric Naval Forces and National Research Council. *Information Assurance for Network-Centric Naval Forces*. Washington, DC: The National Academies Press, 2010. Accessed March 28 2014. http://www.nap.edu/catalog/12609.html.

Crowell, Richard M. *War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare*. Defense Technical Information Center. Accessed March 23, 2014. http://www.dtic.mil/dtic/tr/fulltext/u2/a514490.pdf.

Filipe, Derek A. "Energy Change Detection to Assist in Tactical Intelligence Production." Master's thesis, Naval Postgraduate School, 2009.

Greenert, Johnathan. *CNO's Sailing Directions*. September 23, 2011. Accessed March 28, 2014. http://www.navy.mil/cno/cno_sailing_direction_final-lowres.pdf.

Hart, Dennis J. "An Approach to Vulnerability Assessment for Navy Supervisory Control and Data Acquisition (SCADA) Systems." Master's thesis, Naval Postgraduate School, 2004.

Hughes, Wayne P. *Fleet Tactics and Coastal Combat*. Annapolis, MD: Naval Institute Press, 2000.

Landon, J. P. “Made in China.” *Proceedings Magazine* 137, no. 298 (April 2011). Accessed February 22, 2014, http://www.usni.org/magazines/proceedings/2011-04/made-china.

Lawson, Stephen and Robert McMillan. “FBI Worried as DoD Sold Counterfeit Cisco Gear: By Tampering with Networking Equipment, Spies Could Open up a Back Door to Sensitive Military.” InfoWorld. Accessed February 22, 2014. http://www.infoworld.com/d/security-central/fbi-worried-DOD-sold-counterfeit-cisco-gear-266.

Markus, John and Paul J. DeLia. “Jamming.” AccessScience. Accessed March 22, 2014. http://accessscience.com/content/Jamming/358300.

Roughead, Gary. “CNO Guidance for 2011.” 2010. Accessed March 23, 2014. http://www.navy.mil/features/CNOG%202011.pdf.

Sulmasy, Glenn. *The National Security Court System: A Natural Evolution of Justice in an Age of Terror*. Oxford: Oxford University Press, 2009.

Tester, Rodrick A., “Risk of Cyber Attack to Naval Ships in Port Naval Station Everett: A Model Based Project Utilizing SIAM.” Master’s thesis, Naval Postgraduate School, 2007.

U.S. Marine Corps, U.S. Department of the Navy, and U.S. Coast Guard. *Cooperative Strategy for 21st Century Seapower*. Accessed March 28, 2014. http://www.navy.mil/maritime/MaritimeStrategy.pdf.

“Written Congressional Testimony of the Honorable Ray Mabus Secretary of the Navy February 24, 2010.” 2010. Accessed March 28, 2014. http://www.navy.mil/navydata/people/secnav/mabus/posture_statement_2010.

# INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California